S. HRG. 114–204, PT. 5

DEPARTMENT OF DEFENSE AUTHORIZATION FOR APPROPRIATIONS FOR FISCAL YEAR 2016 AND THE FUTURE YEARS DEFENSE PROGRAM

HEARING

BEFORE THE

COMMITTEE ON ARMED SERVICES
UNITED STATES SENATE

ONE HUNDRED FOURTEENTH CONGRESS

FIRST SESSION

ON

S. 1376

TO AUTHORIZE APPROPRIATIONS FOR FISCAL YEAR 2016 FOR MILITARY ACTIVITIES OF THE DEPARTMENT OF DEFENSE, FOR MILITARY CONSTRUCTION, AND FOR DEFENSE ACTIVITIES OF THE DEPARTMENT OF ENERGY, TO PRESCRIBE MILITARY PERSONNEL STRENGTHS FOR SUCH FISCAL YEAR, AND FOR OTHER PURPOSES

PART 5
EMERGING THREATS AND CAPABILITIES

APRIL 14, 2015

Printed for the use of the Committee on Armed Services

S. HRG. 114–204, PT. 5

DEPARTMENT OF DEFENSE AUTHORIZATION FOR APPROPRIATIONS FOR FISCAL YEAR 2016 AND THE FUTURE YEARS DEFENSE PROGRAM

HEARING

BEFORE THE

COMMITTEE ON ARMED SERVICES
UNITED STATES SENATE

ONE HUNDRED FOURTEENTH CONGRESS

FIRST SESSION

ON

S. 1376

TO AUTHORIZE APPROPRIATIONS FOR FISCAL YEAR 2016 FOR MILITARY ACTIVITIES OF THE DEPARTMENT OF DEFENSE, FOR MILITARY CONSTRUCTION, AND FOR DEFENSE ACTIVITIES OF THE DEPARTMENT OF ENERGY, TO PRESCRIBE MILITARY PERSONNEL STRENGTHS FOR SUCH FISCAL YEAR, AND FOR OTHER PURPOSES

PART 5
EMERGING THREATS AND CAPABILITIES

APRIL 14, 2015

Printed for the use of the Committee on Armed Services

Available via the World Wide Web: http://www.fdsys.gov/

U.S. GOVERNMENT PUBLISHING OFFICE
24–522 PDF WASHINGTON : 2017

For sale by the Superintendent of Documents, U.S. Government Publishing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON ARMED SERVICES

JOHN McCAIN, Arizona, *Chairman*

JAMES M. INHOFE, Oklahoma
JEFF SESSIONS, Alabama
ROGER F. WICKER, Mississippi
KELLY AYOTTE, New Hampshire
DEB FISCHER, Nebraska
TOM COTTON, Arkansas
MIKE ROUNDS, South Dakota
JONI ERNST, Iowa
THOM TILLIS, North Carolina
DAN SULLIVAN, Alaska
MIKE LEE, Utah
LINDSEY GRAHAM, South Carolina
TED CRUZ, Texas

JACK REED, Rhode Island
BILL NELSON, Florida
CLAIRE McCASKILL, Missouri
JOE MANCHIN III, West Virginia
JEANNE SHAHEEN, New Hampshire
KIRSTEN E. GILLIBRAND, New York
RICHARD BLUMENTHAL, Connecticut
JOE DONNELLY, Indiana
MAZIE K. HIRONO, Hawaii
TIM KAINE, Virginia
ANGUS S. KING, JR., Maine
MARTIN HEINRICH, New Mexico

Christian D. Brose, *Staff Director*
Elizabeth L. King, *Minority Staff Director*

Subcommittee on Emerging Threats And Capabilities

DEB FISCHER, Nebraska, *Chairman*

KELLY AYOTTE, New Hampshire
TOM COTTON, Arkansas
JONI ERNST, Iowa
THOM TILLIS, North Carolina
LINDSEY GRAHAM, South Carolina
TED CRUZ, Texas

BILL NELSON, Florida
JOE MANCHIN III, West Virginia
JEANNE SHAHEEN, New Hampshire
KIRSTEN E. GILLIBRAND, New York
JOE DONNELLY, Indiana
TIM KAINE, Virginia

CONTENTS

APRIL 14, 2015

DEPARTMENT OF DEFENSE AUTHORIZATION FOR APPROPRIATIONS FOR FISCAL YEAR 2016 AND THE FUTURE YEARS DEFENSE PROGRAM

TUESDAY, APRIL 14, 2015

U.S. SENATE,
SUBCOMMITTEE ON EMERGING
THREATS AND CAPABILITIES,
COMMITTEE ON ARMED SERVICES,
Washington, DC.

MILITARY CYBER PROGRAMS AND POSTURE

The subcommittee met, pursuant to notice, at 2:35 p.m. in room SR–222, Russell Senate Office Building, Senator Deb Fischer (chairwoman of the subcommittee) presiding.

Committee members present: Senators Fischer, Ayotte, Ernst, Tillis, Nelson, Gillibrand, and Donnelly.

OPENING STATEMENT OF SENATOR DEB FISCHER, CHAIRWOMAN

Senator FISCHER. Good afternoon. The hearing will come to order.

The subcommittee meets today for its annual posture hearing on military cyber programs. And I'd like to welcome all of our witnesses today, and thank each and every one of you for your very honorable service to this country.

Our hearing will be structured in two panels. First, we will hear from Mr. Eric Rosenbach, the Principal Cyber Advisor to the Secretary of Defense, and Lieutenant General Kevin McLaughlin, the Deputy Commander of U.S. Cyber Command. Then, after we do a few rounds of questions, we will ask each of the cyber component commanders to provide their opening remarks and also respond to the committee's questions.

Given the number of witnesses, we ask that everyone keep their remarks to 5 minutes. And your full written testimony will be included in the record.

While the hearing today is the fourth Senate Armed Services hearing on cyber this Congress, it is the first of what I hope will be many engagements for our Subcommittee on Emerging Threats and Capabilities. I thank our witnesses for being here today, and I look forward to their testimony.

With that, I would ask that the full text of my opening statement be entered into the record without objection.

[The prepared statement of Senator Fischer follows:]

PREPARED STATEMENT BY SENATOR DEB FISCHER

The subcommittee meets today for its annual posture hearing on military cyber programs. I'd like to welcome all of our witnesses today, and thank them each for their honorable service.

Our hearing will be structured in two panels. First, we will hear from Mr. Eric Rosenbach, the principal cyber advisor to the Secretary of Defense, and Lieutenant General Kevin McLaughlin, the deputy commander of U.S. Cyber Command. Then, after a couple rounds of questions, we will ask each of the cyber component commanders to provide their opening remarks and answer some questions. Given the number of witnesses, we ask that everyone keep their remarks to five minutes. Your full written testimony will be included in the record.

The chairman of the Joint Chiefs recently stated that the United States enjoys a significant military advantage in every domain except for the cyber sphere. In cyber, “we don't have an advantage,” Chairman Dempsey stated, “and that makes this chairman very uncomfortable.” Those sobering remarks should make all of us very uneasy. Confronting our cyber challenges should be among our highest priorities. I look forward to hearing from our witnesses on how they plan to effectively train, arm, and equip our 6,200 person Cyber Mission Force with the necessary level of urgency.

We have a lot to be proud of—finding resources for a new mission is challenging, especially in times of limited budgets. I commend the Department of Defense, the Services, and Cyber Command for their accomplishments to date. However, much work remains to be done to ensure that the cyberwarriors we are training have the capabilities, tools, and infrastructure necessary to deter and defeat those seeking to exploit our cyber assets. I am concerned that while we have made great progress in creating more defensible networks and building the cyber mission teams, we have lagged behind considerably in developing the capabilities and policy necessary to impose costs on our adversaries. This hinders our ability to deter those seeking to exploit the United States through cyberspace.

To illustrate my concern, consider the fact that the fiscal year 2016 budget request includes $5.5 billion in cyber investments. Unfortunately, when you dig a little deeper into that request, it appears that only 8 percent of that $5.5 billion is allocated for Cyber Command and the training and equipping of our Cyber Mission Forces. These teams are expected to be the backbone of the Department of Defenses cyber capability: guarding the DOD network, supporting our warfighters' requirements in cyberspace, and defending the nation from cyberattack when authorized to do so. We must ensure that these forces are provided with adequate ftlnding to meet the expectations placed upon them. Otherwise, we run the risk of having 6,200 well-frained individuals who lack the capabilities necessary to deter and defeat our adversaries—or, as Chairman McCain put it, a “hollow cyber force.”

Last month, during our full committee posture hearing for U.S. Cyber Command, Admiral Rogers testified that the United States is “at a tipping point where we not only need to continue to build on the defensive capability, but we have got to broaden our capabilities” so that policy makers and military leaders are equipped with an adequate range of options. I am eager to hear how each of you plan to meet the urgent need for offensive military cyber capabilities, and whether the current budget request is sufficient to meet the challenges we face.

Not a day goes by where we don't hear of a bad actor frying to use cyberspace to steal data, impose their will through coercion, or threaten our critical infrastructure. The Cyber Command's written testimony last month was quite sobering. It stated that potential enemies may be “leaving cyber fingerprints on our critical infrastructure” in order to send a message about its vulnerability. Our adversaries are using their cyber capabilities to deter us, and in many respects they are succeeding. It is necessary to signal to those looking to harm the United States that the consequences of doing so will greatly outweigh any perceived benefit. I look to each of your helping us to understand what cyber capabilities will be necessary to impose costs, reverse these troubling trends, and establish better deterrence in cyberspace.

While the hearing today is the fourth Senate Armed Services hearing on cyber this Congress, it is the first of what I hope will be many engagements for our Subcommittee on Emerging Threats and Capabilities.

I thank our witnesses for being here today, and I look forward to their testimony.

Senator FISCHER. I would like to welcome the Ranking Member of the committee, Senator Nelson from Florida, to offer any remarks he may have.

STATEMENT OF SENATOR BILL NELSON

Senator NELSON. Thank you, Madam Chairwoman.

Welcome. We are obviously at a critical juncture. There's a real cyber threat out there. This Senator certainly has a concern that, despite all of the alarms that have been raised about the cyber threat, we still don't seem to be taking it very seriously.

Not long ago, Admiral McConnell, the Director of National Intelligence and NSA as well as the head of Cyber Command, stated his belief that foreign adversaries could bring down the grid on the East and West Coasts through cyber attack. Recently, I received a briefing from well-informed industry experts that were tasked in a national security staff-sponsored cyber threat exercise. And what they briefed me is that a relatively small group of knowledgeable people could bring down the economy of this country in 3 days. They could wreck the Internet and other critical infrastructure systems in this country in relatively short order. Now, such forecasts are made despite the standup of Cyber Command and assurances about how well it's progressed in its ability to protect the country.

It's still hard for us to get the U.S. Chamber of Commerce to come in behind any legislation involving cyber security except that which would be entirely voluntary on the part of the business community. And, in light of these real-life cyber attacks, it seems to me that offense in cyber has the sort of advantages that ballistic missiles have enjoyed over missile defenses for over a half a century, and that cyber weapons can have the effects like weapons of mass destruction.

So, I'm concerned that, in the case of cyber, we are not being honest with ourselves, or the American people, that effective defenses are practical and within the reach of our military in the near term. Specifically, I'm concerned that Cyber Command inherited a strategy from NSA signals intelligence from that culture that has significant limitations in the context of military operations.

Our intel agencies always strive, appropriately so, to know everything about an adversary's capabilities. And, in cyber, that means gaining knowledge of the other side's malware and, whenever possible, their intentions for executing attacks. The hope is that NSA and Cyber Command will reliably have such full insight and can take effective action. But, it's unreasonable, in this Senator's view, to rely so heavily on the success of our intelligence operations to anticipate attacks, especially in an area like cyber, where technology enables adversaries to be quite elusive and to be able to go on the offense without us having a sufficient defense. We must assume that determined adversaries will be resourceful enough to keep secrets from us and to achieve significant surprise. And I don't expect that we're going to have the capability to completely neutralize our adversaries' cyber force, given that computers are cheap and easy to replace, and that the Internet is a vast domain in which to hide and maneuver.

And so, this then brings up the issue of deterrence. Our critical infrastructure is vulnerable, but at least there is deterrence with folks like Russia and China, because they have a lot to lose, as well, knowing that we could respond offensively with a large-scale attack on their economic targets.

So, it's just like the ICBMs of years ago, mutual assured destruction. But, what about the rogue nations or rogue elements—North Korea, Iran, and so forth? And we've certainly had examples of that already—the Sony attacks, *et cetera*.

And so, I want to know from our witnesses if you would agree that deterrence in these circumstances may not be really possible. After Cyber Command's creation, we are finally fielding trained military forces to execute operations. We're about halfway towards our force goals. But, these forces are, to a significant degree, in this Senator's opinion, hollow, in that we are not yet able to equip them with the tools they need to function effectively. We're in a situation, although understandable—a flawed assumption is that military cyber operations would be an extension of NSA's SIGINT activities, including utilizing the same tools and infrastructure. And, while NSA has always, obviously, got to be a critical partner for Cyber Command, it's now understood that this Command needs a different set of capabilities.

And so, I want to get into that, Madam Chairwoman, as we get into our discussion.

And if you guys can't answer the questions, then let's go into a classified setting.

Thank you, Madam Chairwoman.

Senator FISCHER. Thank you, Senator Nelson.

We do plan to have two panels today. And we'll keep track of questions that you gentlemen are unable to answer in an open setting, and then we will go to a classified setting after that.

But, welcome, again, to the subcommittee. If you have your opening statements ready, we will accept those at this time

Mr. Secretary, if you'd like to begin, please. Welcome.

STATEMENT OF HONORABLE ERIC ROSENBACH, PRINCIPAL CYBER ADVISOR TO THE SECRETARY OF DEFENSE

Mr. ROSENBACH. Thank you very much, Madam Chairwoman, Ranking Member Nelson. I really appreciate the opportunity to testify here before the subcommittee to you and other members of the subcommittee.

And I'm also very happy to be with Lieutenant General McLaughlin, the Deputy Commander. He's a very good partner in all this, along with the services, who are working hard.

I think that I don't need to spend a lot of time telling you about the cyber threat landscape, as Senator Nelson just explained. But, over the past several years, we've seen that this is growing, both in sophistication and urgency. When you look at something like the Sony cyber attacks or other things, attacks just against our own DOD networks, we recognize that we need to take this very seriously, both from the state and the nonstate perspective.

Another thing that is really important to highlight, though, is that we're very realistic, from the Department of Defense (DOD) perspective, that this is a team sport, that we do not actually have the lead for all domestic cyber security, that DHS is the lead for many aspects; we need to partner with the FBI; and, just as you mentioned, Senator Nelson, that the private sector has a very important role in protecting themselves. We do have a key role, though. And I'll talk a little bit more about that.

I would like to tell you a little bit about the way we think about deterrence, because this is critically important to our thinking. And, in light of the evolving nature of the threat, DOD is committed to a comprehensive, whole-of-government cyber strategy to deter attacks. This strategy depends on the totality of U.S. actions, to include declaratory policy, overall defensive posture, effective response procedures, indication and warning capabilities, and the resilience of U.S. networks and systems.

Within this, we have three specific roles within the U.S. Government, from a deterrence perspective:

First, we need to develop capabilities to deny a potential attack from achieving its desired effect.

Second, the United States must increase the cost of executing a cyber attack. In this regard, DOD must be able to provide the President with options to respond to cyber attacks on the United States, if required, through cyber and other means. So, something that I would like to emphasize is, although it's a cyber attack, we don't think about the response purely through a cyber lens. It would be all the tools of foreign policy and military options.

And finally, we have to ensure that we're resilient, so, if there is an attack, that we can bounce back. This, when it comes down to it, is pure cost-benefit-type analysis to make sure that the costs are much higher than the benefit to the adversaries who want to attack us. But, again, I have to be very candid that some type of attacks are much easier to deter than others. In the case of nation-states, those are easier to deter. As you mentioned, sir, the Chinese and the Russians, easier to deter—much easier to deter than the North Koreans or the Iranians, and, some of the lower-level criminal attacks or the theft of intellectual property, the most difficult, as I know you all understand.

In order to bolster this deterrence strategy in the Department, we've made the conscious decision to invest in capabilities, and the Cyber Mission Force in particular, that allow us to improve our deterrence posture. So, we have built robust intelligence. I do think that it's an important part of it, although not the core part. I would agree with Senator Nelson on that. And we know that we need to reduce the anonymity in cyberspace so that adversaries who attack us don't think that they can get away with it, that we know who they are, that they will be identified, and we'll be able to take action. These attribution capabilities have increased significantly in recent years, and we continue to work closely with intelligence and law enforcement to improve this.

I just want to remind you all, there are three important missions that we have in DOD:

The first, and our most important mission, is for us to defend our own DOD networks. I know that may be surprising. When you think about the Department of Defense, we're very network-reliant and network-centric, the largest enterprise network in the world. All of our military operations depend on our network. And that's why Cyber Command's first job is to defend DOD networks. The Secretary makes that very clear.

Second, we need to defend the Nation against significant cyber attacks. This is a small part of all the cyber attacks against the United States. This is not a denial-of-service attack, unless it would cross the threshold of armed attack, for most instances. Right? The Department of Defense is not here to defend against all cyber attacks; only that top 2 percent, the most serious.

And then, finally, we want to provide full-spectrum cyber options to the President or the Secretary in cases where that would be advantageous to our National interests.

To carry out these missions, we're building a Cyber Mission Force which is composed of 133 teams. I can tell you more details about that. But, I want to emphasize, too, that there's an important role for the National Guard and Reserves. We want to capitalize on the expertise that folks who are in the private sector but still want to serve the country have. And we've already worked with the services to allow some force structure on that. And developing this talent in a cadre of cyber experts is very important to the Secretary. Since Secretary Carter has been here, it's one of his top priorities, is ensuring we have new tunnels through which talent can come into the Department and cyber and other ways.

Again, to show that we're thinking very clearly about this, next week we'll release a new strategy for the Department that will guide the way forward for the next several year in cyber. The Secretary has driven this, he's very action-oriented, with projects, milestones, and things that we'll be able to measure our effectiveness on. And I'm more than happy to tell you all some about that today, and a lot more in the future, next week.

Also, I just want to emphasize how important building strong partnerships is—with the private sector, with our other government agencies, and with allies and partners. The geography of the Internet itself means that we can't do this alone, and we've invested a lot of time, even recently, in Asia, the Gulf, and other places in the Middle East, and, of course, with our traditional allies, the five allies, and in NATO, in this area.

So, in conclusion, I think it's also important to emphasize that the role that Congress plays in this is very important, both in passing legislation, like the information-sharing legislation, or cyber security legislation that improves the standards of cyber security. Up until now, we've had a very good relationship with the Senate Armed Services Committee and your staff. We want to be very helpful. I look forward to that continuing over the next several years.

With that, I'd request that I could submit my written record for—or, my written testimony for the record, and turn the podium over to Lieutenant General McLaughlin.

[The prepared statement of Mr. Rosenbach follows:]

PREPARED STATEMENT BY HONORABLE ERIC ROSENBACH

Chairman Fischer, Ranking Member Nelson, and members of the Subcommittee, thank you for inviting me to discuss Department of Defense (DOD) efforts in cyberspace. It is my honor to appear today with my colleague from U.S. Cyber Command, Lieutenant General McLaughlin. Cybersecurity is an increasingly urgent and important topic in today's interconnected world, and I appreciate the opportunity to explain the Department's mission in this space and how we continue to improve America's cybersecurity posture.

With respect to cyberspace, DOD continues to focus on its three vital missions: (1) defending DOD information networks to assure DOD missions, (2) defending the Nation against cyberattacks of significant consequence, and (3) providing cyber support to contingency plans and operations. Today, we face diverse and persistent threats in cyberspace that cannot be defeated through the efforts of any single organization. Although DOD maintains robust and unique cyber capabilities that we use to defend our networks and the Nation, we must continue to work closely with our partners in the Federal Government, the private sector, and in countries around the world to ensure we have the necessary strategies, policies, capabilities, and workforce in place to succeed.

THE CYBER THREAT LANDSCAPE

We live in a wired world, and despite the convenience that connectivity brings, it also makes robust cybersecurity more important than ever. State and non-state actors are conducting cyber operations for a variety of reasons, expanding their capabilities, and targeting the public and private networks of the United States, its allies, and partners. These cyber threats continue to increase and evolve, posing greater risks to the networks and systems of the Department of Defense, our national critical infrastructure, and U.S. companies and interests.

External actors probe and scan DOD networks for vulnerabilities millions of times each day, and over one hundred foreign intelligence agencies continually attempt to infiltrate DOD networks. Unfortunately, some incursions—by both state and non-state entities—have succeeded.

Malicious actors are also targeting U.S. companies. At the end of last year, North Korean actors attacked Sony Pictures Entertainment in the most destructive cyberattack against the United States to date. North Korea destroyed many of Sony's computer systems, released personal and proprietary information on the Internet, and subsequently threatened physical violence in retaliation for releasing a film of which the regime disapproves.

Cyberattacks also pose a serious threat to networks and systems of critical infrastructure. The Department of Defense relies on U.S. critical infrastructure to perform its current and future missions. Intrusions into that infrastructure may provide persistent access for potential malicious cyber operations that could disrupt or destroy critical systems in a time of crisis. Because of these severe consequences, DOD is working with our partners in the interagency and private sector to ensure these systems are better protected.

At DOD, we are also increasingly concerned about the cyber threat to the companies in our Defense Industrial Base. We have seen the loss of significant amounts of intellectual property and sensitive DOD information that resides on or transits Defense Industrial Base systems. This loss of key intellectual property has the potential to hurt our companies and U.S. economic growth, but also enables adversaries to more easily achieve technological parity with us.

In light of these evolving threats, DOD is committed to a comprehensive, whole-of-government cyber deterrence strategy to deter attacks on U.S. interests. This strategy will depend on the totality of U.S. actions, to include declaratory policy, overall defensive posture, effective response procedures, indications and warning capabilities, and the resiliency of U.S. networks and systems.

Fundamentally, however, deterrence is largely a function of perception, and DOD has three specific roles to play within a whole-of-government deterrence strategy. First, DOD must develop cyber capabilities to deny a potential attack from achieving its desired effect. If our adversaries perceive that they are not going to succeed in conducting an attack they will be less inclined to act. Second, the United States must increase the cost of executing a cyberattack. In that regard, DOD must be able to provide the President with options to respond to cyberattacks on the United States if required, through cyber or other means. As the President has said, the United States reserves the right to respond to cyberattacks at a time, in a manner, and in a place of our choosing. Finally, we must ensure our systems are resilient, and able to withstand and recover quickly from any potential attack on our own networks. Within DOD, it is our responsibility to make our own systems resilient. Nationally, we support other agencies of the government, like the Department of Homeland Security and the National Institute of Standards and Technology, in fostering effective resiliency measures for the country as a whole.

To support our deterrence posture, DOD is investing significantly in our Cyber Mission Force to conduct cyber operations. Underpinning the Cyber Mission Force, we have built robust intelligence and warning capabilities to reduce anonymity in cyberspace and identify malicious actors' tactics, techniques, and procedures. Our attribution capabilities have increased significantly in recent years, and we will continue to work closely with the intelligence and law enforcement communities to maintain effective attribution capabilities.

DOD'S EVOLVING CYBER STRATEGY AND THE FUTURE CYBER WORKFORCE

As I have said, the Department of Defense has three primary missions in cyberspace: (1) defend DOD information networks to assure DOD missions, (2) defend the United States against cyberattacks of significant consequence, and (3) provide full-spectrum cyber options to support contingency plans and military operations. U.S. Cyber Command (CYBERCOM), as a sub-unified command to U.S. Strategic Command, is responsible for defending DOD networks and defending the Nation from cyber threats, and works in partnership with the combatant commands to conduct full-spectrum cyber operations.

To carry out these missions, we are building the Cyber Mission Force and equipping it with the appropriate tools and infrastructure to operate in cyberspace. Once fully manned, trained, and equipped in fiscal year 2018, these 133 teams will execute CYBERCOM's 3 primary missions with nearly 6,200 military and civilian personnel.

As we continue to strengthen the Cyber Mission Force, we recognize the need to incorporate the strengths and skills inherent within our Reserve and National Guard forces. Each Service, therefore, has developed Reserve component integration strategies that embrace Active component capabilities in the cyberspace domain and leverage the Reserve and National Guard strengths from the private sector. Up to 2,000 Reserve and National Guard personnel will also support the Cyber Mission Force by allowing DOD to surge cyber forces in a crisis. When called upon, these surge forces will serve as a robust DOD-trained force to help defend national critical infrastructure.

As Secretary Carter has said several times in the last month, the development of a cadre of cyber experts—both in and out of uniform—is essential to the future effectiveness of U.S. cyber capabilities, and we are committed to ensuring the workforce for the cyber domain is as world class as the personnel in other warfighting domains. To that end, we are developing and retaining a workforce of highly skilled cyber security specialists with a range of operational and intelligence skill sets. This cyber workforce must include the most talented experts in both the uniformed and civilian workforce, as well as a close partnership with the private sector. Achieving robust capabilities will require long-term planning and investment to ensure that a pipeline of cyber security talent is available to benefit the Department of Defense and the Nation as a whole.

Over the past several years, DOD's approach toward cyberspace has continued to evolve and mature. As such, the Department is in the process of finalizing a new, updated strategy, which will guide DOD's activities in cyberspace in defense and support of U.S. national interests. Once approved by the Secretary, we plan to conduct a series of briefings and discussions with Members of Congress and their staffs. This strategy builds upon our previous cyber strategy from 2011, the national security missions and objectives of the 2014 National Security Strategy, the 2014 Quadrennial Defense Review, and the 2011 International Strategy for Cyberspace.

BUILDING STRONG PARTNERSHIPS

Successfully executing our missions in cyberspace requires a whole-of-government and whole-of-nation approach. DOD continues to work with our partners in other Federal Departments and agencies, the private sector, and countries around the world to address the shared challenges we face. We work particularly closely with our partners in the Department of Homeland Security and Department of Justice to ensure collaboration in cyber operations and information sharing across the Federal Government, and we have seen tremendous advancement in our ability to work as a single, unified team.

Additionally, Secretary Carter has placed a particular emphasis on partnering with the private sector. We need to be more creative in finding ways to leverage the private sector's unique capabilities and innovative technologies. The Department does not have all the answers, and working with industry will be critical to ensuring our technical military advantage in the future. We are examining ways to expand our collaboration with industry and developing incentives and pathways to bring more cyber expertise into the Department.

Finally, our relationship with Congress is absolutely critical. As the President has said many times, congressional action is vital to addressing cyber threats. I appreciate the early steps taken during this session to build consensus on information sharing legislation, and await progress on other key provisions, such as data breach and cyber criminal provisions, included in the President's legislative proposal submitted earlier this year.

CONCLUSION

Cyber threats are real, serious, and urgent, and we can only overcome them with a cohesive, whole-of-government approach. We have made significant strides, but there is still more work to be done. I look forward to working with this committee and the Congress to ensure that DOD has the necessary capabilities to keep our country safe and our forces strong. Thank you again for the attention you are giving to this urgent matter. I look forward to your questions.

Senator FISCHER. Thank you, Mr. Secretary.

General.

STATEMENT OF LIEUTENANT GENERAL JAMES K. MCLAUGHLIN, USAF, DEPUTY COMMANDER, U.S. CYBER COMMAND

General MCLAUGHLIN. Madam Chairwoman and Ranking Member Nelson, thank you very much for having us here today. It's a pleasure to be before you.

It's an honor to also testify with Mr. Rosenbach, our Principal Cyber Advisor to the Secretary of Defense.

And it's an honor to be able to tell you a little bit about what's happening at U.S. Cyber Command, to represent the hard work of the men and women that are in our Command, and so you could hear a little bit about what their focus is today.

I think that, both in your opening comments and in Mr. Rosenbach's, a discussion of threat is sort of paramount. And I think what I'd, maybe, just add to that is, what's different today, on the military side, is commanders. Whereas, before they might have thought of the threat as a nuisance or something where maybe, you know, people were conducting espionage against the United States, realize that, today, the cyber threats are actually something that could actually threaten their ability to command and control their forces and put at increased risk to their ability to accomplish their mission, and that—the Sony attacks are a great example, and it's not lost on them that, today, destructive attacks could occur against, you know, their own cyber terrain, making it difficult or impossible for them to accomplish their mission. So, the threat, in that context, is not just important to U.S. Cyber Command, but it's important to the Department, you know, writ large.

The—so, the real—the issue is, What are we doing about it? And so, the creation of U.S. Cyber Command, again, as Senator Nelson kind of went through a little bit of our history, we've been around just a little bit over 4 years. We are about halfway into the fielding of our Cyber Mission Force, which are the 133 teams, which are a significant way of bringing capacity and capability to bear in our ability to defend the United States and to accomplish Department of Defense missions in cyberspace.

Admiral Rogers, as—in addition to the three missions that Mr. Rosenbach laid out that U.S. Cyber Command has—has really laid out a vision that—where we have four imperatives within our Command aimed at getting after the challenges that have already been laid out today and that I think we'll discuss in more detail.

The first is to defend our Nation's vital interest in cyberspace. We don't do that alone. As was mentioned, our primary lane in the road is to defend our Department of Defense networks and then to bring military capabilities to military commanders. But, we do know that, as part of a broader team with other parts of the government, with the private sector and with our allies, there is a much broader strategic mission that's really on the plates of Americans and our allies. And that's, How do we deal with the threats, more broadly, to the Nation? And that is a key part of this first imperative.

Second, we have to operationalize this mission set. There was a early part in Senator Nelson's comments about early focus, perhaps, on approaches that might align themselves with the intelligence business. And we know we're dependent on intelligence in this area, but what we have to focus on is bringing an operational mentality to this space. This is not just an IT-focused endeavor. This is an operational domain. And so, we are bringing the same operational mindset and processes that we would see in any of the other domains. That's a critical transition, culturally and from a mindset perspective, to how we think about operations in military cyberspace.

Third, we have to integrate cyberspace operations in support of joint-force-commander objectives. A key part of the capacity and capability that we're going to bring is there to support the operations of other commanders, noncyber-focused commanders. And so, a key focus for us is to make sure we integrate and we bring capacity to all the combatant commanders around the globe, and that they have a place to turn for cyber capability, whether it's defensive or offensive in nature.

And then, last, accelerate towards full-spectrum capability. We have to have the ability not just to do—to defend our networks. That's critical. Not just to command and control cyber forces. But, we have to be able to bring full-spectrum capabilities, including offensive capabilities, to bear if we're going to be a full command, able to meet the challenges of our Nation.

All of these forces, as we bring them into being, will also have to be trained and brought to a high level of readiness. And so, you wouldn't expect a fighter wing or a carrier strike group or a brigade combat team to ever go into combat if it hadn't been fully trained and certified as ready to conduct its warfighting mission. And so, a major focus for us will to be to make sure that the forces that we have are also brought up to that same level of readiness and that, when they are asked to go into combat, that—you know, that the commanders understand that they're certified and they're able to do their job.

It is a real privilege to be here with you today. I would like to thank the committee for its strong support, and the Congress for their support, in this area. This open testimony is important for us to actually—just to make sure that these important issues are both understood by, you know, the rest of the military as well as the American people that are watching this. We look forward to working with you as partners, help operationalize the cyber domain, and to make, you know, the challenges that we're faced a little bit less daunting in the future.

Thank you.

Senator FISCHER. Thank you, General.

We will start with 6-minute rounds. And I will begin, for either of you gentlemen to answer.

In the President's fiscal year 2016 budget in dealing with cyber investments, he has $5.5 billion in that budget, but yet we only are looking at 8 percent of that going to Cyber Command and the development of the Cyber Mission Forces. Do you think that's sufficient?

Mr. ROSENBACH. Ma'am, I'll take that first.

I'd say we need to be careful when we look at the cyber budget, because, although maybe 8 percent—and I'm not sure about that number—of the 5.5 billion is going directly to CYBERCOM, there's a lot of money that goes indirectly, through NSA or through DISA or through other places, that ends up supporting them. So, NSA is a combat-support agency. There are lots of things they do to support CYBERCOM.

That said, in the Department and in a fiscally constrained environment, cyber is one of the only three areas where it's either held or grown over the last several years. And the Secretary has made very clear that it's an area that will continue to receive increased growth, and the vast majority of that is for Cyber Command. So, the bottom-line answer is, we even assess that 8 percent is not enough and that there should be some additional growth, and that's part of the strategy, moving forward.

Senator FISCHER. Can you give us any examples of what's needed to more efficiently and effectively provide training?

General MCLAUGHLIN. So, ma'am, what we have on the training side—let me first tell you what we have, and what it is that we still need—one thing that we do have is, as we were directed to bring on the 133 teams, each of the services—and you'll be talking with some of those component commanders in a little bit—were asked to build capacity, really almost overnight, to be able to produce, you know, young enlisted and young officers that could come onto these teams. That part of the training's going great. They went from a standing start, doubled, and then really doubled again their capacity to build those people that are the initial accessions onto these teams.

The place that we still have work to do, and we're pursuing it with vigor, is what we call the persistent training environment. And that is the ability now to take those teams, once the people show up, and—like we would in—you know, in any other warfighting domain—and have the ability for those teams, either subsets of teams or entire teams, to do training against—routinely—against, you know, live adversaries, like aggressor forces, to be able to do mission certification or mission rehearsal events, and to sort of train throughout a continuum from the time they show up until the time they might have to deploy or do their COMINT job.

Senator FISCHER. Right.

General MCLAUGHLIN. That part——

Senator FISCHER. I'll speed you along a little bit on that.

On—but, when we're looking ahead, can you say, in this setting, what you feel will be needed in the future?

General MCLAUGHLIN. Yes, ma'am, I'd—what's going to be needed in the future is, we need to have a couple of components. We need to have a range environment, so the virtual environment for these forces to do training. It needs to be interconnected throughout the United States. We need to have aggressor—you know, forces that replicate the adversary so that there's someone to train against. We have to have people that actually manage and sort of write training scenarios and scripts. So, it's all the components that make up the capacity to train our forces.

Senator FISCHER. You mentioned, General, earlier, about the readiness and the force structure. How do you measure that? Where do you come up with, say, the number 6200? How do you measure that at all?

General MCLAUGHLIN. Well, ma'am, the initial sizing of the Cyber Mission Force, I think, was really put together to—with an estimate of the amount of offensive and defensive capacity we thought we needed as a Department.

Senator FISCHER. Have you been able to, I guess, verify that number, or are you still in the process of estimating what you need on that for readiness and to be prepared and just moving forward? Where are you on that?

General MCLAUGHLIN. Ma'am, I would say that we are primarily focused on taking the forces that have been allocated to us and, on the readiness side, to make sure those forces are trained and ready. I don't—I wouldn't say that we've done a lot of analysis up to this point to determine: Is—are 133 teams the right number, or enough? We're mostly trying to take those teams and make sure that they're ready to do their job.

Senator FISCHER. So, you can't say, at this point, if that number would be adequate.

General MCLAUGHLIN. No, ma'am. But, I also wouldn't be able to say that it's not adequate. You know, our view right now is, we're only halfway fielding the teams. So, I think we would have to get them all the way fielded and have them at full operational capability to be able to do reasonable analysis as to whether or not there's sufficient resource there.

Senator FISCHER. When you look at the question of deterrence—and, Mr. Secretary, I appreciated your comments on that, that it wouldn't necessarily be a cyber response to a cyber attack—but, do you think, at this point, our adversaries view an attack on either government agencies or the private sector—but, let's focus on government agencies—do you think they're—they view an attack right now as low risk for a high reward?

Mr. ROSENBACH. Ma'am, I'd say it really depends on what type of attack. I would say they probably do view it as low risk, when it comes to the exploitation and trying to steal data. I would say it's considerably a higher risk if they were to conduct a destructive attack against a DOD network, for example. The deterrence level there is much higher, and I think they see that as high risk, which is what we go for.

Senator FISCHER. Thank you.

Senator Nelson.

Senator NELSON. Thank you, Madam Chairwoman.

Obviously, NSA is going to be a critical partner for Cyber Command. And I think it's pretty well, however, understood that Cyber Command needs a different set of capabilities: command and control, operational planning, situational awareness, battle damage assessment, mission execution, network infrastructure, weapons.

Mr. Secretary, do you agree that Cyber Command lacks robust joint computer network infrastructure to execute military cyber campaigns effectively?

Mr. ROSENBACH. Yes, sir, they currently do not have a robust capability.

Senator NELSON. Well, what are the attributes of the needed infrastructure?

Mr. ROSENBACH. Sir, I can go into a lot more detail in a closed session. But, I would say, here, that the ways we think about this depend on offense or defense. In defense, I think we have pretty robust capability, and we're in good shape, but could be better. And I think big data analytics could make that even stronger, something we're calling the "unified platform," bringing that together. On offense, Secretary Carter, when he was Dep Sec Def, made the decision and put money against a more Title 10-specific infrastructure that would be for military options, that goes after a platform and access and a payload, to put it in very simplistic terms. But, I can talk to you a lot more about that in a classified session.

Senator NELSON. Okay. Do you agree that Cyber Command lacks a robust command-and-control platform and systems to plan and execute fast-moving and large-scale cyber operations?

Mr. ROSENBACH. Yes, sir, I agree with that.

Senator NELSON. You agree that Cyber Command itself does not have the resources or expertise to build this cyber command-and-control infrastructure and weapon systems.

Mr. ROSENBACH. At this point, sir, I think that the question of resources is one where we have added resources in those areas. And, because we're trying to be very smart about attacking a very difficult technical problem, we're doing it in a measured way to be good stewards of government money. These are very hard technical problems. And, rather than invest a large amount of money before we're sure, we're kind of taking that incremental approach, but are working towards it. And, I think, when we see success, the Secretary, in particular, will be willing to invest more in it.

Senator NELSON. Well, if you don't have the resources, do you think that the military services will have to do this?

Mr. ROSENBACH. Sir, there's no doubt the Services play a huge role in this. And I say this very honestly, that what they've done, thus far, has been great, and they will continue to play a key role in——

Senator NELSON. I'm sure. But, we're trying to help you, here. So, are the Army, Navy, and Air Force prepared to step up and budget for these joint requirements?

Mr. ROSENBACH. It depends on the service, but, in large part, the services are stepping up, although, in a tough environment like we have right now, it's very hard for them to allocate existing resources to cyber. And so, one of the things that we're looking at is whether there should be new resources for the services.

Senator NELSON. So, you're not even to the point of allocating the task to each of the services.

Mr. ROSENBACH. It depends on what the task is, sir. But, here's why we haven't specifically allocated tasks to each of the services.

There is as big decision to make about the model that we want for CYBERCOM. And, essentially, it comes down to this. Is CYBERCOM going to be more like SOCOM, with those types of authorities and that type of model, or is it going to be something closer to now that is much more reliant on service-generated man/train/equip and the capabilities, in particular? That's a decision we're thinking very consciously about, but have not yet made.

Senator NELSON. And that's the lack of a policy decision that has been made. And so, does Cyber Command have the resources and the expertise to at least produce operational requirements?

Mr. ROSENBACH. I think it depends. And, honestly, I'd prefer that you ask General McLaughlin for his perspective on that so that I'm not answering too much for the Command on that.

Senator NELSON. Well, let me ask you. If you're lacking in this area, which you've already said, basically, that you don't have the budget for it, how is the Secretary—what should the Secretary of Defense do to provide the needed support?

Mr. ROSENBACH. I guarantee you this, sir, that Secretary Carter really cares about cyber. He's taking it very seriously. And if we see that there's a need for additional resources, he would be the first one to put them there.

The other thing I would say is, it's nothing against CYBERCOM, but it's a young command. It's nascent and it's still growing. And it does take a very highly developed human-capital base to make acquisition decisions, to run programs, things that, traditionally, the services have done. And that's why we're thinking so carefully through this.

Senator NELSON. In your planning, do you plan to hit nonmilitary targets?

Mr. ROSENBACH. Sir, I can tell—I can touch a lot more detail in a closed session. But—yes, but in a very, very precise and confined way that would always adhere to the Law of War and all the things we think about for collateral damage and other targeting. And I'm sure General McLaughlin could add more to that; in particular, in a classified environment.

Senator NELSON. Such as, if, for example, that you wanted to take out the enemy's air defenses, you could go in and knock out the power stations, the civilian power stations.

Mr. ROSENBACH. Sir, you know, I think talking in a classified environment would be better for specifics. And then I can go into great detail about things like that.

Senator FISCHER. Thank you, Senator Nelson.

Senator Ernst.

Senator ERNST. Thank you, Madam Chairman.

Thank you, gentlemen, for being here today.

This past weekend, I had a very exciting drill, in that we, in the Iowa National Guard, spent some time discussing our 2016 Vigilant Guard exercise. This is exercise play which will involved Federal agencies, of course the Iowa Army and Air Guard, as well as State agencies, local agencies. It's a series of—the play will include a series of weather and natural disasters, but also including cyber attack and security issues. And it is something that we have recognized at all levels in the government in Iowa, that this is a very real possibility.

So, I appreciate you stepping up. I know that the Command is new, but I look forward to those challenges and opportunities that we have in developing that. And I am excited about the 17 series cyber branch bringing on officers and new soldiers into that area. I will tell you, in the Guard, we have a great number of members that would quite adequately fill into those types of activities.

Admiral Rogers, I believe, on March 4th before the House Armed Services Committee, he did state that there—in quote, "There's no DOD solution to our cyber security dilemmas. The global movement of threat activity in and through cyberspace blurs the U.S. Government's traditional understanding of how to address domestic and foreign military, criminal, and intelligence activities.

And, with that being said, the National Defense Authorization Act (NDAA) for Fiscal Year 2014 directed the President to develop an integrated policy to deter adversaries in cyberspace and to provide that cyber deterrence policy to Congress within 270 days. And that deadline has come and gone, and we have not seen that policy. Considering that we see a continuously evolving threat to our cybersecurity, this failure to present a deterrence policy places our country at risk. And again, we're seeing that at all levels, in all places of the United States.

And, to Senator Nelson's point, we talked a lot about budgeting, but it's very difficult to budget when you don't know what the administration's policy is. When you talk about SOCOM-type activities versus other types of activities, we don't know, we don't have a policy.

And so, I would just ask, Mr. Secretary, is there something that we're not aware of that is stopping the President from providing this policy? Are there some hurdles that we need to overcome? What do we need to do to get that policy?

Mr. ROSENBACH. Yes, ma'am. First of all, I'd just like to say I've met with the Iowa TAG several times to talk about cyber issues. Very smart guy. And I also—my mom would kill me if I didn't say I spent my summers in Lake Okoboji, so I know about Iowa.

[Laughter.]

But, that's—yes, ma'am, but that's not to butter you up and to not admit that we're not late on the——

[Laughter.]

—the deterrence report that you mentioned.

The interagency and the White House has led an effort. That report is almost entirely finished. We've put a lot of thought into it. And, just because I'm in the Pentagon, I'm not able to say exactly when it would come to you. But, I want to emphasize that that's more of a report. The overall deterrence policy is something in—a cyber operations policy that the National Security Council has put forward and does play into our thinking, in a large degree.

So, I wouldn't want anyone to think that there's not a lot of deep thinking about deterrence in the U.S. Government, but particularly in DOD.

Senator ERNST. Okay. Well, I appreciate that. And, yes, you did butter me up. Okoboji is lovely. So, you're welcome back anytime.

Yes, and General Orr is very intent on making sure that we have a very realistic exercise play, this upcoming year. And so, we are excited about this opportunity.

So, as we continue to develop the cyber deterrence policy, what are some of the challenges that you are facing right now? Senator Nelson has brought up a number of challenges that are out there, SOCOM versus other types of activities. What are those challenges? And do you see anything that we, as legislators, can assist you with in that aspect?

Mr. ROSENBACH. Thank you, ma'am. I'll sort of answer quick and then let General McLaughlin say it.

The biggest challenge, quite frankly, when we think about deterrence, is making sure that we deter enough that the attack doesn't come, but we don't escalate things to the point that we bring more attacks upon ourselves. So, it's really important to remember that the United States is a glasshouse when it comes to cyber, and we need to be really careful how much we do things like think about going on offense, because that almost inevitably will lead to more attacks on us. So, that's why we think about using other tools in the toolbox, like economic sanctions or other aspects of military show of force, from my perspective.

But, I think General McLaughlin has thoughts on this, too.

General MCLAUGHLIN. The key thing on the—from the Cyber Command perspective, ma'am, on the deterrence piece, is really making sure we deliver the capabilities that are part of deterrence. It's defendable networks—make sure that we get those networks fielded so that the adversary doesn't think he just has an easy target and doesn't tempt them to use their capability. Today, I think we are—we could be an easy target, because we haven't fielded that defendable terrain. Getting our teams not only fielded, but, as was mentioned—Mr. Rosenbach mentioned things like the unified platform or Title 10 tools and infrastructure—we think of those sort of as enablers.

And so, we need to get the enablers crisply defined and fielded so that you have people plus the capability, whether you consider them the weapons or the infrastructure. It's the kit that our teams—that these component commanders behind me, that their teams need to actually be able to have a robust capability. I think, from—on the deterrence piece, that's what we really bring to the table at Cyber Command, will be the military forces that can be an element of deterrence, certainly not the—certainly not everything that's required to deter.

Senator ERNST. Thank you. My time is expired.

Thank you, General. Thank you, Secretary.

Thank you, Madam Chairman.

Senator FISCHER. Thank you, Senator.

And Senator Tillis.

Senator TILLIS. Thank you, Madam Chairman.

Thank you, gentlemen, for being here today.

One quick question is, How does any of the funding you receive—how is it threatened by sequestration?

Mr. ROSENBACH. Sir, I'm going to give you one specific example and then turn to General McLaughlin so he can give you more detail.

During sequestration in the past, it put a big hole in the training pipeline for these Cyber Mission Forces. And what we saw is, because we had to turn off schoolhouses, there was as big impact on the rate of development for the overall Cyber Mission Force. And it really has hurt us in a way that makes me nervous. And, if that were to happen again, we'd be even further behind in developing the capability——

Senator TILLIS. And, Secretary——

Mr. ROSENBACH.—the capabilities like that.

Senator TILLIS. Mr. Secretary, that, as the human capital you need to execute the mission, can you give me a rough idea, in terms of a percentage of the pipeline that you would have liked to have had versus was affected by sequestration—a rough idea of what that is?

Mr. ROSENBACH. I think, honestly, General McLaughlin can give you more details on that, and even more on the impact.

Senator TILLIS. Okay.

General MCLAUGHLIN. So, sir, we're roughly 50 percent through the fielding of those 133 teams, and we are—we're supposed to have all of them at initial capability by the end of fiscal year 2016. So, we literally have a quarter of the additional teams that are in the build just for—in this, in the next fiscal year. So, sequestration will make—will put a big dent on the ability of the Services to produce the people that we need to fill out those teams.

Senator TILLIS. What about the—some of the longer-term investments that you have to make while we're in this budget mode of living paycheck to paycheck? What sorts of long-term strategic investments are out there that you would like to make that are impossible to make on 12-month investment horizons?

Mr. ROSENBACH. Sir, Secretary Carter recently has emphasized that sequestration is one of those things where it's actually a waste of money, for the reason that you note, is, we're not able to do long-term planning, so you make poor investment decisions based on a shorter time horizon.

For some of the big rocks, as CYBERCOM calls them—so, the persistent training environment, a unified platform—those are things that are a more significant investment that we think much harder about whether or not we would allocate resources to when we're unsure of how much will actually be there.

Senator TILLIS. You all were mentioning that your top priority is the 2 percent of, I think, DOD or defense- related cyber attacks that you see. Is that—did I hear that correctly?

Mr. ROSENBACH. Yes, sir. It's not exactly 2 percent. Only to show—for the biggest threats to the Nation are the ones in that defend-the-Nation mission that we try to prevent or deter.

Senator TILLIS. What about the sort of macro threat? If I were—I worked in the private sector and did ethical hack testing and tried to find ways to penetrate businesses—large businesses and—you know, if I were on the cyber battlefield, I wouldn't necessarily go after the ones where I know it's going to hurt most if I get caught. To lead up to your capacity to do that, I'd go after the downstream supplier base for DOD. I'd go after municipalities and government institutions to disrupt a broader population so that you have a whole lot of things that you have to look at before I would get to a level—I mean, are we looking at threats in that way? And do we have resources marshaled in that way? Because that transcends into the private sector and the U.S. Government supply base, which is large and diverse.

Mr. ROSENBACH. Yes, sir, that's a great question. There are two ways, in particular, that we've been watching this as it relates to DOD. So, the first is, we know that a lot of the defense contractors have been penetrated and intellectual property pulled out. And so, we're trying to use new contracting mechanisms. And the SASC has been very helpful in this in passing some aspects of the law to make it better so that the private sector has sort of upped their game. Then, second, TRANSCOM, we've seen, has been penetrated by some adversaries—the Chinese, in particular—who know that, by going to the supply chain, they may be able to hit us at a weaker point than going directly there. And that's something that SASC also did some reports on that were helpful. So, those are the two ways.

And then, in the more general private sector, it's an even more difficult situation, because it's a significant investment for a lot of the private-sector firms.

Senator TILLIS. I don't think I'll get to this question, but I would like to speak with you all at some point about, How do we look at the underlying infrastructure through which all these cyber attacks occur? And are we looking at ways to, maybe, look ahead to an architecture that makes it still maintain the privacy considerations, but find better techniques or a better underlying infrastructure for authentication so that it puts you in a better position to defend and potentially attack?

But, I had a final question that has more to do with—I love what the Commandant of the Marine Corps said at a SASC meeting a couple of months ago. He says he never wants to put an American soldier in a position to where he or she is going into a fair fight. And I think, for most of our men and women in uniform, we've got the strategies to do that. But, it seems to me that, in this realm, we have adversaries out there that, on any given day, although our sophistication may be slightly better, there are certain battlefields where it could just be a fair fight and we could get—we could be harmed as much as we could do harm. Is that a fair assessment?

Mr. ROSENBACH. Sir, I think it's a fair assessment, just given the asynchronous, asymmetric nature of cyber. And General McLaughlin probably has some thoughts on that, too.

General MCLAUGHLIN. Well, I think, because of the diverse nature of the threats against us, including threats that operate in ways that we wouldn't operate as a Nation—it's just not in our character—I do think you could see the potential where it might not look—where it might look like it's a fair fight, you know, at least today. And so, I think our goal is—at least within the DOD side—is to make it where it's not fair, you know, to bring these capabilities to bear that we're—that we've been discussing, so that our military forces, in particular, don't have to go into conflict, in the future, thinking about this is going to have be a fair fight.

Senator TILLIS. Thank you.

Senator FISCHER. Thank you, Senator Tillis.

Senator Gillibrand, I know you just arrived. Would you—are you ready for your questions? Okay, thank you.

Senator GILLIBRAND. Thank you, gentlemen, for being here. Appreciate your service and your hard work.

CYBERCOM obviously has a wide array of responsibilities. How do you deal with unexpected threats? And do you have the capabilities to meet those threats? And, in the event of a cyber attack, would you need an additional surge capacity?

General MCLAUGHLIN. Ma'am, I think the ability to deal with unexpected threats, and then surge them, requires a—some attributes that I think that we are building. First is the ability to be flexible, to be able to move resources from one set of challenges to another. We've seen the need for that, just in the recent 12 months. You know, we've seen things, like the Sony attack, we've seen resurgent issues with regard to Russia. So, we've seen issues where our Department has made, including the cyber, adjustments in priority. So, being flexible and agile to respond to things that perhaps you weren't forecasting is something that's built into our model.

But, you raise a great point on the ability to surge. So, we are building a set of forces—we've talked a little bit about them today—133 cyber teams that are going to be the basic capacity and capability for our military forces in Cyber. What we've also added, though, are forces in the total force. So, all the services have constructs for their Reserve Forces. And the Army and the Air Force have—with their Guard forces, are actually going to be brought online and actually provide capacity for the Nation if they needed to be called up. You could surge and bring even more military capacity with the total force. That is part of our construct. It's just really been defined in about the last 12 months, and now both the Reserves and the Guard are building their teams, certified to the same standards that the Active Duty teams will have. And that will be additional resource if there was a surprise or a need to surge resources to an emergency.

Senator GILLIBRAND. And what's your vision, with regard to Guard and Reserve components, for CYBERCOM?

General MCLAUGHLIN. Our vision, from the Cyber Command perspective, was very clear. We wanted to make sure that all Reserve and Guard forces were able to be trained to the same standard so that, if they were called up to do the Title 10—you know, to support in a Title 10 status—they would be equal and capable.

Senator GILLIBRAND. So, you're envisioning equivalent training.

General MCLAUGHLIN. Yes, ma'am.

Senator GILLIBRAND. Okay.

General MCLAUGHLIN. Absolutely. And that they would be able to also be commanded and controlled in a seamless, the same way that the Active-Duty Forces would—you know, would be commanded and controlled.

So, that's the—that's really the—from the Cyber Command perspective, what we laid out. Each of the Services has taken a slightly different way that they've—that they are thinking about integrating Reserve and Guard forces into their structure. They all fit within our construct at Cyber Command. And I know each of the—those component commanders in the second panel would be glad to talk to you about specifically what's unique about each Service, in terms of how they think about their——

Senator GILLIBRAND. And will that change after fiscal year 2016? Would you still be able to—the people assigned to CYBERCOM would still be able to receive the same training?

General MCLAUGHLIN. Yes, ma'am. Our plan is that this—that's the steady-state——

Senator GILLIBRAND. Okay.

General McLaughlin:—mode that we would like to be in.

Senator GILLIBRAND. And then, representing New York, obviously, we have a lot of emerging threats to our infrastructure, to our financial markets, and to basic national security. And I've met with a lot of the experts in the field there. What are your thoughts on the relationship and the coordination between Homeland Security and DOD, in terms of cybersecurity and role responsibilities? And, more to the point, do you see—what do you see as the Department of Defense's role in the support of States, DHS, and the FBI?

Mr. ROSENBACH. I'll take that one, ma'am.

I think—it's been interesting for me, because I've been in the Department for almost 4 years now, working on cyber issues. And when I first came, there was a lot of tension between DOD and DHS, and a little struggle about who would have the lead. It's completely different now. The relationship is very strong. We know that DHS/FBI have the lead for domestic issues. We then will come in behind them and support them, very often. You could ask General McLaughlin, if you want, for example, about the support that DOD and NSA gave during the Sony cyber attacks in a domestic way.

And then, the relationships between the State and local governments usually is through DHS, just like defense support for civil authorities. In all ways, we need a lead Federal agency, and then we can provide support to them or to the States.

Senator GILLIBRAND. Now, if you are doing this level coordination and training, do you have the resources and support you need to do those missions?

Mr. ROSENBACH. Ma'am, you know, because the cyber threat is growing so much, we see that we'll need more resources down the line, and the Department has prioritized Cyber as one of those that will continue to get additional resources.

Senator GILLIBRAND. Do you need any additional authorities?

Mr. ROSENBACH. Right now, there are none that we think we need, but we've always worked real closely with the Senate Armed Services Committee (SASC) in the past. And I'm sure, if we identified those, that we would—we would welcome your support.

Senator GILLIBRAND. In the issue of recruitment, we've just received a report from all Services articulating their plans either to create separate specialties or designators for cyber. It's my understanding that the training necessary to build a cyber warrior can take up to 2 years. How do you envision the development, not only of separate specialties for cyber, but also career tracks for cyber warriors? How do we retain them and get a return on the investment the United States has put into these warriors?

Mr. ROSENBACH. I'll let General McLaughlin speak in more detail, but I know that's something you've worked a lot on in the past, and been helpful in getting new authority for us. That has been very good. So, I would like to thank you for that, explicitly, and then let General McLaughlin talk more about the details of the training.

General MCLAUGHLIN. Sure. Senator, the—each—as you mentioned, each Service is thinking through what type of specialties and career tracks it needs in the cyber warfare domain. They've all taken slightly different paths, but each of them are—have come up with a path so that you can now come in as a new entry or accession, and you can conceive a career in this area. It's not something you would dabble in or come in and out of.

Senator GILLIBRAND. That's great.

General MCLAUGHLIN. And so, from our perspective, it's not only important that they've done that so that our initial people, as they come in, are qualified, but we actually need, you know, mid-level and senior, you know, people that have deep experience in this. So, the—so, their work to build the career path is critical for us, and it's something we're watching. We've really just sort of laid out the requirement, and each of the Services, you know, strapped on and has, I think, again, taken a slightly different path, but each of them, at the end of the day, are going to have people with that type of—that depth over a career.

Senator GILLIBRAND. Thank you.

General MCLAUGHLIN. The last thing, you mentioned about just—I would just add—keeping them in. So, retention will be a big deal.

Senator GILLIBRAND. Yup.

General MCLAUGHLIN. If you're going to invest 2 years training someone on a set of very, very high-end skills that actually are marketable in the civilian workplace, our job will be to retain them. It's not only to show that they have a valid career, but also if there are incentives or other things that might help offset, you know, the fact that they could make more elsewhere, you'll see us—where each of the Services is looking at that.

And then also flexible models. You know, how can we be flexible in the workforce of the 21st century to let people, you know, feel like they—perhaps we could bring in people from the private sector, or we could do other things, not just use the same model we've always used in the Department.

Senator GILLIBRAND. Thank you.

Senator FISCHER. Thank you, Senator.

We will have a 4-minute round for the second round, here, so we can have our second panel up and still get down to the classified briefing. Senator Nelson would like to meet down there yet today.

So, I'm just going to ask a couple of quick questions, here, Mr. Secretary. One on deterrence again, and then on acquisition, if I can.

When we look at the sanctions that were recently authorized by the President and against the cyber attackers, how do you see that contributing towards better deterrence in cyberspace? And specifically, when you look at the other agencies, when you look at State and you look at Treasury and you look at Justice, are the agencies working together? And how's the Department working with him on that?

Mr. ROSENBACH. Thank you, ma'am. In the case of the Sony attacks, on the sanctions that went against the DPRK, we, as an interagency, looked very, very closely at the organizations we could target with those sanctions that would inflict the most cost on them. So, remember what I talked about, the cost-benefit relationship for deterrence; that's why. So, that, of course, was led by Treasury and other experts in the interagency, but we had as much a voice in that as anyone. And I do think that's something that was effective and has impacted the decision calculus of the North Koreans.

Senator FISCHER. When we have a show of force in other domains, that can have a stabilizing effect, I believe, on a situation that may be deteriorating out there. How important do you think it is that we be able to do that within the cyber realm?

Mr. ROSENBACH. Ma'am, I think, honestly, most countries around the world know that we have capability in cyber and could demonstrate that force. I personally don't think that it would be wise to demonstrate it unless we really needed to, because I'm very worried about how vulnerable we are and that someone would then follow our example and just try to show the United States that they could also take down part of the infrastructure to demonstrate that. So, I think a cautious approach, where we're conservative and we try to keep things stable, is quite important.

Senator FISCHER. A lot of times, we hear that cyber is similar—the—a cyber deterrence is similar to nuclear deterrence. Many people believe that. I question it in many regards. Feel free to correct me on that, but how do you see it?

Mr. ROSENBACH. Without sounding too, maybe, cheeky, I'd say most of the people I hear who say that tend to be from the Cold War era and think that things are very analogous, when, in fact, I don't think they are at all. And I agree with you that the analogy with the nuclear part is not that strong.

Senator FISCHER. I was able to spend some time back in Nebraska, the last 2 weeks, and I spent a day out at STRATCOM and had some briefings on cyber. So, it—it's fascinating what's out there. I appreciate the work you do on that.

With acquisition now. When we look at the latest addition of the better buying power list, cyber security—they're listing that as a new area of emphasis, and they want to elevate that in the acquisition process. What input do you have on that release from Secretary Kendall? How do you see that shaping up?

Mr. ROSENBACH. Yes, ma'am. I work very closely with Under Secretary Kendall. Almost every day, we're in touch. And in my role as the Principal Cyber Advisor, I'm kind of the point guard or the quarterback for things on cyber inside the Department. And so, of course, he's the lead on that. But, it was something that was coordinated even with the Services. And we want to, you know, just strengthen our ability to make some of the defense contractors up their game a little bit in cyber security.

Senator FISCHER. And when you look at the acquisition process, I mean it takes forever, right? So, when you're looking at cyber and you're looking at technology, how are you going to speed that up in order to, I mean, truly meet the needs that are there before what you're trying to acquire becomes out of date in 18 months and you haven't even gotten through the process?

Mr. ROSENBACH. That's a great question. And I assure you, Secretary Carter's interest in accomplishing exactly that is very passionate, and he's put a lot of pressure on everyone in the Department to do better. Next week, he is going to Silicon Valley and will give a speech. That's one of the topics that he's going to address to try to push us to do better in that area and build more bridges with the private sector. Silicon Valley, just one example.

Senator FISCHER. Great. Thank you.

Senator Gillibrand.

Senator GILLIBRAND. Can you just describe—it came up in the last hearing, that we're going to be doing some recruiting for Guard and Reserve in Silicon Valley—can you describe what that program's going to look like?

Mr. ROSENBACH. Ma'am, I can't give too many details, because I don't want to unveil the gift before it comes next week in the speech, but we've been thinking a lot about ways we can get new pipelines or tunnels of talent into the Department from kind of nontraditional places. So, the Guard is another place where, in going and traveling and visiting some of the Guard units, I've recognized there really are people who, for example, work for Microsoft and still work in the Guard in Washington State. That's just one way, but we would also like to try to find other ways in the Department where you don't have to go into one of the Services, for example. So, we're thinking a lot about that. Silicon Valley is a natural place. New York and around New York City, another place. There are a couple of places like that, where we're looking at centers of excellence.

Senator GILLIBRAND. So, once it's public, can you send me a letter describing the program?

Mr. ROSENBACH. Yes, ma'am, I will absolutely do that. I promise I'm not trying to be evasive. I'm just trying to——

Senator GILLIBRAND. No, I know. I just—I'm interested, so I want to know.

Mr. ROSENBACH. I will. We'll send you the full report. And I can brief your staff——

Senator GILLIBRAND. To the extent you need any support for that program in this NDAA, let me know and we will write it.

Mr. ROSENBACH. Great. Thank you.

Senator GILLIBRAND. So, any substantive language needs to be added about authorities or funding, this year's NDAA would be the appropriate place to try to put that in.

Mr. ROSENBACH. Yes, ma'am, thank you.

Senator GILLIBRAND. Continuing on, on the issue of sort of the dynamic threat environment, how do you address the fact there's continually morphing requirements and distinct threats that face both the DOD and the United States as a whole? How do you plan for it? How do you model for it? How do you stay ahead of it?

Mr. ROSENBACH. I'll say, very generally, and then I'd like General McLaughlin's thoughts, is, we try to build a very capable force that is dynamic enough that it can shift. And, with that, I think he can give you the best answer.

General MCLAUGHLIN. Yes, ma'am. I think if we spend our time trying to predict exactly what the threat is going to be or how it will manifest itself, we'll end up guessing wrong. So, our job is to field forces that both technically are trained at a very high level, you know, they have a lot of technical skills, and they've been given a flexible set of capabilities so that—and that we have great intelligence—you know, we'll need great intelligence capabilities, as well—so that, if something occurs, and it will, that we didn't forecast, we don't have to retool our force, you know, create new capabilities. We actually can take the people and the capabilities we've fielded and rapidly put them against some new or emerging threat.

Senator GILLIBRAND. And I assume you're also training for offensive acts.

General MCLAUGHLIN. Yes, ma'am. I would mean that for both our defensive and our offensive teams.

Senator GILLIBRAND. And you probably need to answer this in the closed setting, but can you describe a little bit where you feel the threats are, whether they're lone-wolf threats or they're state-actor-driven threats, or if it's really a balance of both? If you need to Reserve that for closed setting, you can.

General MCLAUGHLIN. Yes, ma'am. I think to address it in depth, it would be better in closed hearing, but I will tell you they span the range from the Nation-state-level threats to—you know, to the lone wolf or—

Senator GILLIBRAND. But, do you see either one more of a growing threat or more of a risk?

General MCLAUGHLIN. I think they're all threats, but I would say the place to bring the most capacity are nation-state-level threats.

Senator GILLIBRAND. State actors, yeah.

General MCLAUGHLIN. Yes, ma'am.

Senator GILLIBRAND. Thank you.

Thank you, Madam Chairwoman.

Senator FISCHER. Thank you, Senator.

Thank you, gentlemen. Hopefully, a little after 4:00, we'll meet you down in the SCIF for a classified session. Thank you so much.

And, with that, I would ask that panel two step forward, please. And I apologize, to you folks, that we have a brief time for your presentation.

On our second panel, we have Lieutenant General Cardon, who is the Commander, U.S. Army Cyber Command; Vice Admiral Tighe, Commander, U.S. Fleet Cyber Command; Major General Wilson, Commander, Air Forces Cyber; and Major General Daniel O'Donohue, Commanding General of the U.S. Marine Corps Forces Cyberspace.

So, welcome, gentlemen. I would——

And, I'm sorry, ma'am. It's so good to see you.

Welcome, to all of you. And I would ask that, if you would have very brief opening remarks, Senator Gillibrand and I, then, will ask questions and give you an opportunity to respond to those.

So, Major General O'Donohue, would you like to begin, please?

STATEMENT OF MAJOR GENERAL DANIEL J. O'DONOHUE, USMC, COMMANDING GENERAL, U.S. MARINE CORPS FORCES CYBERSPACE

General O'DONOHUE. Madam Chairwoman, it's an honor to appear before you today on behalf of your marines and their families. Thank you for continued support to our growing cyber capability.

During this dynamic period of transition, it's especially important that we receive budget capability on time, as well as flexible support for still developing manpower, acquisition, and training initiatives.

As a component of U.S. Cyber Command and in full partnership with our sister Services and agencies, Marine Force Cyber is ready to conduct full-spectrum cyberspace operations. Specifically, we provide the joint force specialized cyber teams in a dedicated joint force headquarters. In our component role, our worldwide cyberspace operations are primarily in support of SOCOM. This reinforces a broader relationship, in keeping with the Marine Corps' role as a global crisis-response expeditionary force and readiness. In our service role, the Commandant set a clear priority to fully integrate cyberspace operations into the already multi-domain approach for our marine air/ground task forces and naval expeditionary forces. This involves a reset of our networks based on operational principles and innovative manpower model or challenging readiness standards and a supporting IT strategy that includes operationally responsive acquisitions. Commanders at every level seek competitive advantage in air, land, sea, and cyberspace, with a combined-arms approach, in concert with maneuver, intel, command and control, kinetic and nonkinetic fires. Commanders should be able to contain and defeat adversaries in cyberspace while simultaneously operating across all other domains with potentially degraded but still resilient command and control.

To that end, we are fielding the cyber forces required by our strategy—ready, on time, and with increasing interoperability—in ways we have not imagined. Even before units are fully manned, trained, and equipped, we are achieving operational outcomes as these teams support current operations in stride with their fielding.

We defend against advance threats through active deterrence, hardening of our networks, realistic training, and exercises in high-fidelity cyber ranges. Every marine is increasingly trained as a disciplined and opportunistic cyber warrior.

Currently, we are pursuing a joint service strategy for the multiyear development of a unified network that will facilitate command and control, provide real-time situational awareness, and assist with decision support for commanders. Our network will be optimized for operational support to forces as they deploy globally in an unstable and unpredictable security environment. The marines provide a ready, forward expeditionary extension of cyber capability for the joint interagency and combined force.

Thank you for the opportunity to appear before you today and the continued support for your dedicated marines. I look forward to answering your questions.

[The prepared statement of General O'Donohue follows:]

PREPARED STATEMENT BY MAJOR GENERAL DANIEL J. O'DONOHUE, USMC

INTRODUCTION

Chairman Fischer, Ranking Member Nelson, and distinguished members of this subcommittee, it is an honor to appear before you today. On behalf of all marines, our civilian workforce, and their families, I thank you for your continued support.

I appreciate the opportunity to discuss the Marine Corps' cyberspace operations posture.

The Marine Corps is the Nation's expeditionary force-in-readiness. We are forward deployed, forward engaged, and prepared for crisis response. For generations, your marines have been victorious against our Nation's foes by remaining agile and adaptable to dynamic environments and evolving threats. As the force that is 'the most ready when the Nation is least ready,' we are prepared to defend against adversaries who operate across multiple domains to include cyberspace.

Our current operating environment is volatile, complex, and distinguished by increasingly sophisticated threats that seek asymmetric advantage through cyberspace. Our cyberspace posture guards against these threats, while simultaneously exploiting our competitive advantage in employing combined arms to include closely integrated cyberspace operations.

Our joint cyberspace mission builds on the Marine Corps institutional focus as a global crisis response force with strong naval, interagency, combatant command (COCOM), Special Operations Forces, cross-service and coalition partnerships. 2015 is a key transitional year as we deploy rapidly maturing cyber capabilities and make them central to Marine Air Ground Task Force, COCOM and coalition training, planning, and operations. Activities in cyberspace increasingly influence all our warfighting functions.

Marine Forces Cyberspace Command (MARFORCYBER) is engaging in ongoing cyberspace operations, making strong progress with the force build, achieving operational outcomes, and building capacity for tomorrow's opportunities and challenges. Our priorities are to operate and defend our networks, support designated COCOMs with full spectrum cyber operations, organize for the fight, train and equip the cyber workforce, develop workforce lifecycle management, and to ensure mission readiness through joint and service capabilities integration.

MISSION AND ORGANIZATION

As the Service component to U.S. Cyber Command, MARFORCYBER conducts full spectrum Cyberspace Operations to ensure freedom of action in and through cyberspace, and deny the same to our adversaries. The operations include operating and defending the Marine Corps Enterprise Network (MCEN), conducting Defensive Cyberspace Operations (OCO) within the MCEN and Department of Defense Information Networks (DODIN), and—when directed—conducting Offensive Cyberspace Operations (OCO) in support of joint and coalition forces. MARFORCYBER is also designated at the Joint Force Headquarters-Cyber (JFHQ–CYBER) as directed by CYBERCOM.

The Marine Corps is in a period of transition from multiple legacy contractor owned and operated networks to a unified system architecture that is organized according to our warfighting philosophy and doctrine. We are building a naval approach that will enable the warfighting functions for competitive advantage in a complex environment. These unique characteristics give our Service a competitive advantage in an intersecting battlespace.

OPERATIONALIZING CYBER

MARFORCYBER is in its 6th year of operation. Our focus remains developing ready cyberspace capability for the naval, joint and coalition force. Consistent with our Commandant's guidance, we are developing tactical cyber capacity as an organic aspect of how we fight. Marines will increasingly operate and defend in a compromised and degraded environment. We must align our operational readiness standards and risk mitigation to this reality. Our battlefield networks must be resilient, redundant and interoperable, and extend from the garrison environment forward to the tactical edge of battle.

Further, in conjunction with joint and interagency partners, we intend to pursue the development of an integrated and unified platform for cyberspace operations that will enable centralized command and control, real time situational awareness, and decision support. We are accomplishing this through close coordination with industry partners, and aligned with Deparment of Defense (DOD) and CYBERCOM priorities in support of the Joint Information Environment.

TRAIN AND EQUIP

In this presumably automated and system driven arena, our most valuable resource is our people. Just as the Marine Corps remains dedicated to the notion that there is no more dangerous weapon than a Marine and his rifle, we must provide our Marines with the tools and resources they need to defend our Nation. In order to maintain an asymmetric advantage, we must outpace our adversaries' ability to develop and procure those resources. The acquisition process by which we acquire vehicles and aircraft incurs steep opportunity costs when applied to cyber technology and innovation. Our acquisition processes are deliberately procedure heavy and risk averse, to ensure appropriate delivery of viable solutions. Statutory and regulatory changes will be required in order to enable responsiveness to emerging cyber threats and missions. Current acquisition processes do not adequately support the delivery tempo required for emerging cyber solutions. The tempo at which emerging technologies must be acquired to meet cyberspace operational mandates is occurring at a much greater pace, which creates tension within the acquisition process. We must strike a balance between rapid acquisition to meet emerging threats and changing operational demands and maintaining disciplined engineering rigor of enterprise networks. Adaptability and flexibility are critical to ensuring our cyber mission force teams are ready.

MARFORCYBER's approach to training and developing the cyber work force has a singular vision-to train as we fight. Specifically, MARFORCYBER will adapt a persistent training environment to support training and exercises of cyber units that are assigned to conduct military cyber operations. This training environment will be designed to enhance military occupational skills (MOS} proficiency, test and development of next generation solutions, host remote training and education of Marine Corps Operating Forces, and refine tactics, techniques, and procedures (TTPs) to increase effectiveness of cyberspace operations. Additionally, we are developing a web based training environment hosted by Carnegie Mellon University Software Engineering Institute, a Federally Funded Research and Development Center (FFRDC). This environment combines extensive research and innovative technology to offer a new solution to cyberspace operations workforce development. The focus of this collaboration is to help practitioners and their teams build knowledge, skills, and experience in a continuous cycle of professional development. The combined effect of this approach is for cyberspace operations workforce to train individually and collectively. This initiative will support the future development and certification of Cyber National Mission Forces (CNMF) training requirements.

We have dramatically increased cyber integration into the training cycle by leading, supporting, or participating in over 31 combined, joint, and Marine Corps exercises in the past year. Commanders across our Marine Corps are asking for cyber capabilities both in real world operations and in training to ensure their marines are ready to face the challenges presented by a shifting complex landscape.

WORKFORCE LIFE-CYCLE MANAGEMENT

We have seen substantial increases in capacity and capability. Such achievements are significant but they have not been easy, and MARFORCYBER's success grows from the hard work of its people. Marines and civilians have shown a sharp interest in pursuing a cyber career.

Since 2012, we have dramatically increased our workforce-with an authorized strength of almost 1,000 marines and civil servants today. By the end of fiscal year 2016, MARFORCYBER's authorized strength will increase to over 1,300 personnel, which is in line with previous projections. The majority of these new personnel are allocated to support the cyber mission force as directed by the Secretary of Defense.

In order to attract and retain the best people, the Marine Corps has followed multiple lines of effort. To improve continuity and reap greater return-on-investment in the lowest density highest demand military occupational specialties (MOS), we have coordinated with our Service to extend standard assignments to 4 years. Additionally, the number of feeder MOS available to lateral move into critical cyber related specialties has been increased in order to obtain a larger talent pool of qualified and experienced Marines. We are currently accessing 16 feeder occupational specialties from the communications, signals intelligence, electronic warfare, data, and aviation specialty fields to meet the personnel demands of cyber occupational field. The largest reenlistment or lateral move bonus offered in the past year of $60,750 was offered to sergeants who move into the Cyber Security Technician specialty. To drive home the point of how seriously the Marine Corps takes its cyber talent management, this bonus consumed 16 percent of the retention bonus budget for the last fiscal year. Furthermore, to ensure we have the right metrics, we are leveraging academia and industry to understand how to better attract and retain talent. In the future, our focus will broaden to include generating a sustainable force generation model that retains a unique, skilled expertise within the larger contexts of cyber ready MAGTFs.

Going forward, the Marine Corps is reviewing its manpower models, and considering new management structures to adapt with the increasingly complex and technical aspects of the security environment in which we operate. Beyond technical training, we will place an increasing emphasis on leaders with experience to shape and mentor incoming talent. Courses of action are being developed today in order to impact our manpower models this summer. In the long term, we will look forward to your assistance in order to reshape this new paradigm.

READINESS

MARFORCYBER is leading the effort to take cyberspace operations mainstream across the Marine Corps so as not to be outpaced in an evolving and complex battlespace. Initial teams are being operationally employed as they achieve IOC. As we support the DOD and CYBERCOM efforts to implement a unified cyberspace architecture of the JIE, we continue to improve the operational readiness of our existing enterprise network (MCEN). We have assumed full control of the MCEN, which was previously contractor-managed, and have decreased our legacy network footprint.

In conjunction with joint, interagency, and private partners, we intend to improve our operational readiness and our ability to measure it. In this context, our staff is working and collaborating with our partners to develop rapid acquisition of tools, training environment, and development of procedures that will allow us to train as we fight.

Last June, CYBERCOM certified our first Cyber Mission Team (CMT) as fully operational (FOC) and simultaneously, our first national Cyber Protection Team (CPT) and the second Cyber Mission Team (CMT) reached initial operational capability (IOC). MARFORCYBER is on track to have over75 percent of its CMT, CPT, and CST teams resourced by the end of fiscal year 2015.

In order to fulfill the requirements of CYBERCOM, we have been actively engaged in building and sourcing our national and combat mission, protection, and support teams (CMT, CPT, CST). With one CMT currently certified, the plan going forward is to have MARFORCYBER's second CMT certified early in calendar year 2015. We have one operational CPT working from the MCNOSC, which is our service wide network operations and security center. Our second CPT, which will be in support of national missions, is in the process of certification now. In addition, we stood up our Joint Forces Headquarters-Cyber (JFHQ–C), now at Full Operational Capability (FOC), which directs and coordinates the actions of cyber forces in support of directed missions. The current glide slope for team build-out is to have two CMTs, three CPTs, and one CST at either IOC or FOC by the end of fiscal year 2015. No later than the end of fiscal year 2017 all teams will be FOC, meaning the Marine Corps will furnish one NMT, three CMTs with one CST in support, and eight CPTs. Three of those CPTs will be dedicated to Marine Corps' specific needs. All other teams will function in support of joint requirements from unified and subunified combatant commands.

CONCLUSION

Over the past 6 years, MARFORCYBER experienced both the increased risk and opportunity presented by a world that grows more connected. These experiences reinforced the need to remain focused on our priorities of developing our organization and cyber workforce, refining our service support to MAGTF operations and joint cyber forces, and securing our networks to yield results for commanders worldwide. Although I am pleased to report that our growth is increasing our capacity, capability, and integration with warfighters, I must reiterate the opportunities and challenges that lie ahead are great. While global technology advances rapidly, the Marine Corps faces challenges in adapting its acquisitions to operate at the speed required of cyberspace. Critically, in this domain characterized by human activity, people remain our center of gravity. Resourcing and sustaining this most valuable asset also remains a difficult task. These are difficult challenges, but through your continued support and leadership, we can count such difficulties among the many that marines have overcome in the defense of this great nation.

Thank you for this opportunity to appear before you today. Thank you for your continued support of our marines and civilians and I look forward to answering your questions.

Senator FISCHER. Thank you, sir.

General Wilson.

STATEMENT OF MAJOR GENERAL BURKE E. WILSON, USAF, COMMANDER, 24TH AIR FORCE, COMMANDER, AIR FORCES CYBER

General WILSON. Madam Chair Fischer and the distinguished members of the panel—of the subcommittee, thank you for the opportunity to appear before you today alongside my component commanders. It's an honor to represent the outstanding men and women of 24th Air Force and Air Forces Cyber.

I'm extremely proud of the work our airmen, officers, enlisted, and civilians do every day to field and employ cyber capabilities in support of combat and Air Force commanders.

In the interest of time, let me just share a few examples to highlight how our airmen are making positive, lasting impacts to our Nation.

Last year, the Air Force completed the migration of our unclassified networks from many disparate systems into a single architecture. We transitioned 644,000 users over—across 250 geographic locations to a single network, and reduced over 100 Internet access points to a more streamlined 16 gateways. The end result is a more reliable, affordable, and, most importantly, defensible network, which has been a significant step forward for the Air Force.

The Air Force also championed the fielding of the next generation of technology, known as the Joint Information Environment, by partnering with the Army in the Defense Information Systems Agency. Together, we are implementing joint regional security stacks in modernizing our networks in order to achieve a single DOD architecture. The combined team achieved a critical milestone last fall, when we fielded the first security stack down at Lackland Air Force Base, in Texas. We fielded several more, and continue to push hard. These efforts will benefit the entire Department by reducing our network attack surface and increasing network capacity and capability. We see this as a very significant step.

Like the other Services, we have made significant progress towards fielding and employing our initial Cyber Mission Forces. Today, the Air Force has 15 teams that have achieved initial operating capability, and 2 teams have achieved and have reached full operating capability. In addition to providing unprecedented support to joint and coalition combat forces in Afghanistan and Syria, these cyber forces are engaged in support to combatant commanders and Air Force commanders around the world, as well as defense of the Nation.

I'm proud to report our Air Reserve component is a full partner in the Cyber Mission Force build in addition to our other day-to-day cyber operations. We've leveraged traditional reservists, Air Reserve technicians and Air National Guardsmen across the Command to meet our warfighting commitments. Whether it's providing command and control of our cyber forces from one of our operation centers, deploying as part of our combat communications team, installing cyber infrastructure around the world, or any other task, each of our total-force airmen meet the same demanding standards and serve alongside their Active Duty counterparts. In my humble opinion, it's a tremendous example of the total-force integration at work.

Today, the Air Force also—we've instituted several key initiatives to better recruit, develop, and retain our cyber forces. Most recently, we approved a Strikes for Certifications Program, which provides the opportunity for candidates to enlist at a higher grade when entering the Air Force with described—or the desired cyber-related certifications. We've also continued our selective reenlistment bonus program to provide additional incentives for enlisted members to continue to serve in the demanding cyber and intelligence specialties. For our officers, we have complemented the cyberspace warfare operations career track, which we established several years ago, with our new Cyber Intermediate Leadership Program, which we believe has been key. Our first board competitively selected 83 majors and senior captains to serve in command and operational positions, many as members of the Cyber Mission Force.

And finally, we continue to host a number of initiatives aimed at improving the outreach to our Nation's younger generation. I'd like to highlight just one, if I could, please. It's called Cyber Patriot. And it's sponsored by the Air Force Association, in partnership with local high schools and middle schools around the country, several industry partners, as well as cyber professionals from the Air Force. Cyber Patriot's goal is to inspire students to pursue careers in cyber security or other STEM career fields. In September, we had over 2,100 teams, involving nearly 10,000 students in the United States, Canada, United Kingdom, and our DOD schools around the world. They all began participating in cyber training and competitions. We saw a 40-percent increase in participation, this school year. Cyber Patriot culminated here locally at the National Harbor last month, when 28 teams competed in national finals. Students earned national recognition and scholarships. And, without a doubt, the program is an example of how public/private partnerships can make a real difference. Personally, it's been a rewarding—very rewarding to see our airmen giving back to our younger generation.

These are just a handful of examples of how Air Forces Cyber and 24th Air Force are all-in and fully committed to the mission. Our cyber force is more capable than ever before. We continue to have challenges, but we get better every day.

None of this would be possible without your continued support. It's clear resource stability in the years ahead will be vital to our continued success in developing airmen and maturing our capabilities to operate in, through, and from the cyberspace domain. Simply put, our cyber warriors are professionals in every sense of the word, and they deserve our full support.

Along with my fellow commanders, it's an honor to be here today. Thank you again for the opportunity, and I look forward to your questions.

[The prepared statement of General Wilson follows:]

Prepared Statement by Major General Burke E. Wilson, USAF

INTRODUCTION

Chair Fischer, Ranking Member Nelson, and distinguished members of the subcommittee, thank you for the opportunity to appear before you today, with my counterparts from the other military Services, to discuss Air Forces Cyber's contributions to joint operations in cyberspace. We have made significant strides towards normalizing the Air Force's cyber operations over the last few years. Air Forces Cyber (24th Air Force) is one of four Service Cyber Components established to support U.S. Cyber Command; our headquarters is at Joint Base San Antonio-Lackland, TX, and we have ongoing cyber operations around the world. The outstanding men and women of Air Forces Cyber have been diligently working to increase our capacity and capability to build, operate, defend, and engage across the full spectrum of cyberspace capabilities in, through and from cyberspace in support of joint warfighters. I'm extremely proud of the work they do each and every day in support of military operations around the world, while at the same time, innovating and mastering new and emerging technologies within cyberspace to project global military power.

Cyberspace is an inherently global domain that impacts nearly every function of our Joint Force, which is increasingly dependent upon cyber capabilities to conduct modern military operations. To that end, today's capabilities enable streamlined command, control and execution of joint operations through the rapid collection, fusion, and transmission of information at unprecedented speed, capacity, and precision.

However, the pace of threats continues to grow in scope, intensity and sophistication. Recent attacks such as the Sony Pictures Entertainment incident that resulted in physical damage demonstrate that no industry or sector is immune to this growing threat. State-sponsored actors, non-state-sponsored actors, criminals, and terrorists operating in the cyberspace domain will continue their attempts to penetrate Department of Defense (DOD) networks and mission systems. We must remain vigilant and not falter in our commitment to properly prioritize our support to cyber missions, even with the strain of diminishing resources across the Department.

In response to these growing threats, Air Forces Cyber remains committed to delivering innovative and cost-effective solutions for the joint warfighter with unwavering focus on delivering mission success. Air Forces Cyber's priorities are as follows: employ cyber capabilities in support of combatant and Air Force commanders; develop and empower our airmen and take care of their families; lead through teamwork, partnerships and a strong warfighting narrative; and equip the force through rapid, innovative fielding of cyber capabilities. In this dynamic environment, resource stability will be critical to our ability to protect our networks, provide the needed cyber forces, protect critical information, and provide full spectrum cyber capabilities in support of combatant and air component commanders around the world.

EMPLOYING CYBER CAPABILITIES

Air Forces Cyber has placed significant emphasis on normalizing cyber operations. We continue to transform our organization to an operational Component Number Air Force providing ready cyber forces and capabilities to combatant and Air Force commanders. Our operational level command and control center has made incredible gains towards our ability to effectively integrate the full spectrum of cyber operations and capabilities in support of joint and air component operations.

We cannot stand still in this environment and must continue to build our capability and capacity. Working closely with Air Force Space Command, 25th Air Force (formerly Air Force Intelligence, Surveillance and Reconnaissance Agency), and the Air Staff we have established cyber forces in support of the DOD's approved strategy. In full coordination with our Total Force partners in the Air National Guard and Air Force Reserves, these new cyber teams are providing U.S. Cyber Command with capabilities to defend the Nation, support combatant commanders, and defend the DOD Information Network. We have reorganized our units to meet the training and equipment requirements to build a ready force of approximately 1,700 mission-ready personnel. In concert with the Air Force's basing process, we have identified Joint Base San Antonio-Lackland, TX, as well as Scott Air Force Base, IL, as primary locations for our Cyber Protection Teams. The remaining cyber forces will operate at the National Security Agency's regional operating centers. Today, Air Forces Cyber has 17 operational cyber mission teams—2 fully operational teams and an additional 15 teams that have achieved initial operational status. Our Joint Forces Headquarters-Cyber also declared initial operational status in October 2013 and continues to work toward achieving full operational status.

In 2014, the Air Force designated seven cyberspace systems as weapons systems directly supporting our lines of effort. This designation has been critical to our ability to operationalize and integrate cyber capabilities through a normalized budget, sustainment and support process.

The Air Force has completed the migration of its portion of the DOD Information Network (e.g. the Air Force Information Network (AFIN)) into a single, centrally-managed, and defended architecture. Transitioning over 644,000 users across more than 250 geographic locations to a single network has enabled Air Forces Cyber (24th Air Force) to operate, maintain, and defend a standardized network using centralized control and decentralized execution with more optimally employed resources. Additionally, we've worked tirelessly to collapse over 100 internet access points into a more streamlined and manageable 16 gateways for the Air Force. The end result has been critical to achieving a more effective, efficient, and defensible network.

Finally, our operations center is leveraging a combat-proven joint planning and execution process to command and control our cyber forces. Air Forces Cyber is employing small defensive cyber maneuver forces to complement our enterprise defensive capabilities to identify, assess and mitigate vulnerabilities and adversary actions within our networks. This new approach has proven truly effective in a number of operations over the past year and we continue to make strides in the planning, command, control, and execution of cyberspace operations.

DEVELOP AND EMPOWER OUR AIRMEN AND TAKE CARE OF THEIR FAMILIES

Our innovative airmen are the centerpiece to our Air Forces Cyber capabilities. Therefore, we continue to be wholly committed to recruiting, training, developing, and retaining the right cyber talent. Whether a military or civilian candidate, the Air Force begins by recruiting highly-qualified individuals with demonstrated competency and character.

To meet the growing requirements of the Department of Defense's Cyber Mission Force, the Air Force has restructured and expanded its initial training and force development programs. These changes are yielding significant results and put us on pace to nearly quadruple the rate at which cyberspace operators will be qualified to join Air Force cyber teams in support of the Cyber Mission Force.

Realizing the need to operationalize our training, we have also mirrored our cyber operations training based on lessons from our counterparts in air and space operations. Specifically, we have leveraged the mission qualifications process to ensure our cyber operators meet mission-ready status. Additionally, our cyber operators now participate in U.S. Cyber Command and Air Force Warfare Center events such as Cyber Flag and Red Flag to better hone their skills through real-world force-on-force exercises that provide the ability to integrate cyber capabilities with other domains in a live training environment. Air Forces Cyber's participation in simulated live-fire environments is accelerating the development and fielding of new tactics, techniques and procedures. These cyber warrior's experiences are further magnified when participants bring hard won lessons back to their home units.

Air Forces Cyber's participation in a wide array of combatant command, joint, and Service exercises also complements our efforts to integrate cyber effects with both kinetic and non-kinetic operations across multiple warfighting domains. While demanding in terms of time and resources, these exercises have become integral to effectively developing our airmen into a ready cyber force capable of operating in joint and coalition environments.

To better develop our forces, the Air Force has also instituted a new cyberspace officer career field specific to Cyberspace Warfare Operations to develop airmen with the requisite skills and expertise to meet our Nation's emerging needs. In addition, a Cyber Intermediate Leadership program has been developed to ensure cyber operators and appropriate intelligence officers are provided the right professional growth opportunities in key command and operational positions. The first Air Force board recently convened to review and competitively select officers for these unique leadership positions. In an effort to retain our highly skilled enlisted force, the Air Force offers a selective reenlistment bonus that provides additional incentive to continue to serve our Nation in this emerging mission.

LEAD THROUGH TEAMWORK, PARTNERSHIPS AND A STRONG WARFIGHTING NARRATIVE

Conducting successful operations in cyberspace requires seamless integration with a host of mission partners. In many ways, cyber is a "team sport" and Air Forces Cyber (24th Air Force) is wholly committed to strengthening our relationships with other Air Force partners, our sister Services and interagency counterparts, combatant commanders, coalition allies, as well as civilian and industry partners. Given the proximity of our headquarters and close mission alignment, 25th Air Force continues to be a critical strategic partner across all of our missions. The 25th Air Force Commander, Major General Jack Shanahan, has been a steadfast supporter throughout the standup of the Cyber Mission Forces.

U.S. Cyber Command serves as the focal point for all DOD cyber operations. As one of the four Service Cyber components, we provide an array of cyber forces and capabilities in order to defend DOD Information Networks (DODIN), support combatant commanders, and strengthen our Nation's ability to withstand and respond to cyber events. The recent stand-up of the Joint Force Headquarters DODIN under the leadership of Lieutenant General Hawkins and the Defense Information Systems Agency (DISA) was a major milestone in normalizing the command and control of network defensive operations.

As already highlighted, we partner closely with the Air Reserve component in day-to-day cyber operations. Through a compliment of Traditional reservists, Air Reserve technicians and Air National Guardsmen, our Air Force's cyber units are a striking example of Total Force Integration in action. These total force professionals bring a unique blend of experience and expertise to the full spectrum of cyber missions. Many work in prominent civilian positions within the Information Technology industry, which bolsters our mission effectiveness through their willingness to serve the Nation. Likewise, we are often able to retain unique skillsets gained by investment in our airmen by supporting their continued service in the Air Force Reserves or Air National Guard. These partnerships will be vital to our future operations as the Air Reserve component continues to provide integrated support of the DOD's Cyber Mission Force.

Air Forces Cyber also understands the cyberspace domain is primarily provisioned by private industry and our ability to collaborate with our industry partners benefits the Nation's cybersecurity posture. We have developed Cooperative Research and Development Agreements with industry leaders such as Symantec, AT&T, USAA, Northrop Grumman and 21 other partners to share and collaborate on innovative technologies and concepts. These collaborative efforts allow us to advance science and technology in support of cyberspace operations, as well as share best practices with industry partners. We continue to leverage this program and are currently in the process of enhancing our partnerships with academia.

We also enjoy strong relationships with other DOD components. As an example, the Air Force recently aligned with the Army and the DISA to support the development and fielding of a key technology in the transition to a Joint Information Environment (JIE). Together we are implementing Joint Regional Security Stacks (JRSS) and making enhancements to our networks with Multi-Protocol Label Switching (MPLS) as part of the single security architecture. Through this teamwork, the first JRSS "security stack" was fielded at Joint Base San Antonio-Lackland, TX, in line with 1 of the 16 Air Force Gateways. Additional "security stacks" are being installed at other Air Force and DOD sites as part of the JIE. These efforts [JRSS, MPLS] benefit the entire DOD by reducing attack surface of our networks and threat vectors—allowing for more standardized security of our networks and by providing increased network capacity to support defense missions.

We are also fortunate to have a longstanding, close relationship with San Antonio, TX, also referred to as "Cyber City USA." The local community has committed significant resources to support the growth of cybersecurity both locally and nationally. Our leadership team participates in a variety of civic leader engagements to share lessons related to cybersecurity. The community leadership also understands that encouraging our younger generation to gain the needed cyber skills will be essential to our Nation's success in this arena. By partnering together, Air Forces Cyber (24th Air Force) supports a broad array of programs designed to touch young students. A good example is the Air Force Association's "CyberPatriot" STEM initiative in which our airmen mentor cyber teams as part of a nationwide competition involving nearly 10,000 high school and middle school students. Another example is our "Troops for Teens" program at a local high school focused on reaching over 100 at-risk students through exposure to military values, heritage and way of life. These programs are two of many ways our airmen give back to their communities.

EQUIP THE FORCE THROUGH RAPID, INNOVATIVE FIELDING OF CYBER CAPABILITIES

We are also making gains in improving our acquisitions process to support the ever changing technology of cyberspace. The Air Force Life Cycle Management Center has worked diligently to streamline our ability to provide solutions to support our cyber missions through "Rapid Cyber Acquisition" and "Real Time Operations and Innovation" initiatives. These efforts have resulted in the fielding of capabilities that have thwarted the exploit of user authentication certificates, the unauthorized release of personally identifiable information, and the blocking of sophisticated intrusion attempts by advance persistent threat actors. These technical solutions were developed and fielded in weeks to months.

Similarly, Air Forces Cyber (24th Air Force) is working closely with 25th Air Force to improve our development, fielding, and employment of multi-domain capabilities that leverage the Air Force's unique strengths in cyber, electronic warfare and intelligence, surveillance and reconnaissance. The collaboration is enabling airmen to drive innovative solutions to many of our most challenging operational challenges. It also harnesses the subject matter expertise in other Air Force organizations such as the Air Force Research Laboratory, Air Force Institute of Technology, National Air and Space Intelligence Center, Air University, Air Force Academy, as well as academia and industry to meet growing joint warfighter needs.

CONCLUSION

We are proud of the tremendous strides made by Air Forces Cyber (24th Air Force) to operationalize cyber capabilities in support of joint warfighters and defense of the Nation. Despite the challenge of growing and operating across a diverse mission set, it is clear Air Force networks are better defended, combatant commanders are receiving more of the critical cyber effects they require, and our Nation's critical infrastructure is more secure due to our cyber warriors' tireless efforts. They truly are professionals in every sense of the word.

Congressional support has been essential to the progress made and will only increase in importance as we move forward. Without question, resource stability in the years ahead will best enable our continued success in developing airmen and maturing our capabilities to operate in, through and from the cyberspace domain. Finally, resource stability will foster the innovation and creativity required to face the emerging threats ahead while maintaining a capable cyber force ready to act if our Nation calls upon it.

Senator FISCHER. Thank you, sir.

Vice Admiral Tighe.

STATEMENT OF VICE ADMIRAL JAN E. TIGHE, USN, COMMANDER, U.S. FLEET CYBER COMMAND, COMMANDER, U.S. 10TH FLEET

Admiral TIGHE. Thank you. Madam Chairwoman Fischer and distinguished members of the subcommittee, thank you for your support to our military and for inviting me to appear before you today. I appreciate the opportunity to share with you the Navy's operational view of cyberspace in addition to our initiatives to improve both our cybersecurity posture and operational capabilities as part of the joint cyberspace team in order to address this ever-increasing threat to our Nation and our allies.

Fleet Cyber Command directs the operations to secure, operate, and defend Navy networks within the Department of Defense information network. We operate the Navy network as a warfighting platform which must be aggressively defended from intrusion, exploitation, and attack so that it is both available and trusted for all maritime missions that the Navy is expected to carry out. The Navy network consists of more than 500,000 end-user devices, approximately 75,000 network devices, and nearly 45,000 applications and systems across three security enclaves.

We've transformed the way we operate and defend this network over the past 2 years based on operational lessons learned. Specifically, beginning in summer of 2013, the Navy fought through an adversary intrusion into our largest unclassified network. Under a named operation, known as Operation Rolling Tide, Fleet Cyber Command drove out the intruder through exceptional collaboration with affected Navy commanders, U.S. Cyber Command, the National Security Agency, Defense Information Systems Agency, and our fellow service cyber component commanders.

Although an intrusion upon our networks is always troubling, this operation served as a learning opportunity and has matured the way that we operate and defend our networks and simultaneously highlighted our gaps in cybersecurity posture and weaknesses in our defensive operational capabilities. As a result of this operation and other cybersecurity initiatives inside of the Navy, we have already made, proposed, or planned for a nearly $1 billion investment that greatly reduces the risk of successful cyberspace operations against Navy networks. Of course, these investments are built on the premise that our future real budgets will not be drastically reduced by sequestration.

Specifically, if budget uncertainty continues, we will have an increasingly difficult time addressing this very real and present danger to our National security and maritime warfighting capability.

Operationally on a 24-by-7 and 365-day-a-year basis, Fleet Cyber Command is focused on configuring and operating layered defense and depth capabilities to prevent malicious actors from gaining access to Navy networks, in collaboration and cooperation with our sister Services, U.S. Cyber Command, Joint Force Headquarters, DODIN, DISA, and the National Security Agency. Additionally, we're driving towards expanded cyberspace situational awareness to inform our network maneuvers and reduce our risk. As you know, the Navy and other Service components are building the maneuver elements in the Cyber Mission Force for U.S. Cyber Command by manning, training, and certifying teams to the U.S. Cyber Command standards. Navy is currently on track to have personnel for all 40 Navy-sourced Cyber Mission Force teams in 2016, with full operational capability the following year. Additionally, between now and 2018, 298 Cyber Reserve billets will also augment the cyber force manning plan.

In delivering on both U.S. Cyber Command's and the U.S. Navy requirements in cyberspace, I am fortunate to have fantastic partners, like these component commanders, in addition to many other partner organizations across the Navy, Department of Defense, U.S. Government, academia, industry, and our allies who are every bit a member of our team cyber and critical to our collective capability.

Thank you again, and I look forward to your questions.

[The prepared statement of Admiral Tighe follows:]

Prepared Statement by Vice Admiral Jan E. Tighe, USN

Chairwoman Fischer, Ranking Member Nelson and distinguished members of the xubcommittee, thank you for your support to our military and the opportunity to appear before you today along with my military Service component counterparts and partners.

Madam Chairwoman, I have been in command of U.S. Fleet Cyber Command and U.S. 10th Fleet for just over 1 year. U.S. Fleet Cyber Command reports directly to the Chief of Naval Operations as an Echelon II command and is responsible for Navy Networks, Cryptology, Signals Intelligence, Information Operations, Electronic Warfare, Cyber, and Space. As such, U.S. Fleet Cyber Command serves as the Navy Component Command to U.S. Strategic Command and U.S. Cyber Command, and the Navy's Service Cryptologic Component Commander under the National Security Agency/Central Security Service, exercising operational control of U.S. Fleet Cyber Command operational forces through 10th Fleet. Specifically, we conduct cyberspace operations to ensure Navy and joint or combined forces' freedom of action while denying the same to our adversaries.

The commissioning of U.S. Fleet Cyber Command and reestablishment of U.S. 10th Fleet on January 29, 2010, closely followed the Navy's 2009 acknowledgement of information's centrality to maritime warfighting, known as Information Dominance. Information Dominance is defined as the operational advantage gained from fully integrating the Navy's information functions, capabilities, and resources to optimize decision making and maximize warfighting effects. The three pillars of Information Dominance are assured command and control (C2), battlespace awareness, and integrated fires. U.S. Fleet Cyber Command is a key warfighting element in delivering on missions across those three pillars.

Since my U.S. Fleet Cyber Command predecessor ADM Michael S. Rogers last testified before this subcommittee in July 2012, the Department of Defense (DOD), U.S. Cyber Command, and the Service components have significantly matured cyber operations and enhanced cyber operational capabilities. I appreciate the opportunity to outline the Navy's progress over the past two years, where we are headed to address an ever increasing threat, and how budgetary uncertainty is likely to impact our operations.

CYBER OPERATIONS, POSTURE, AND FUTURE INVESTMENTS

U.S. Fleet Cyber Command directs operations to secure, operate, and defend Navy networks within the Department of Defense Information Networks (DODIN). We operate the Navy Networking Environment as a warfighting platform, which must be aggressively defended from intrusion, exploitation and attack. The Navy Networking Environment consists of more than 500,000 end user devices; an estimated 75,000 network devices (servers, domain controllers); and approximately 45,000 applications and systems across 3 security enclaves.

Operations during the past 2 years led to a fundamental shift in how we operate and defend in cyberspace. Specifically, late summer 2013 we fought through an adversary intrusion into the Navy's unclassified network. Under a named operation, known as Operation Rolling Tide, U.S. Fleet Cyber Command drove out the intruder through exceptional collaboration with affected Navy leaders, U.S. Cyber Command, National Security Agency, Defense Information Systems Agency (DISA), and our fellow Service cyber components. Although any intrusion upon our networks is troubling, this operation also served as a learning opportunity that has both matured the way we operate and defend our networks in cyberspace, and simultaneously highlighted gaps in both our cybersecurity posture and defensive operational capabilities. As a result of this operation and other cybersecurity initiatives, the Navy has already made or proposed (through fiscal year 2020) a nearly $1 billion investment that reduce the risk of successful cyberspace operations against the Navy Networking Environment. Of course these investments are built on the premise that our future year budgets will not be drastically reduced by sequestration. Specifically, if budget uncertainty continues, we will have an increasingly difficult time fully addressing this very real and present danger to our national security and maritime warfighting capability.

The Navy's future cybersecurity investments are being informed by the Navy's Task Force Cyber Awakening, which was chartered by the Chief of Naval Operations and the Assistant Secretary of the Navy for Research, Development, and Acquisition to gain a holistic view of cybersecurity risk across the Navy, and beyond just our corporate navy networks to include combat and industrial control systems. The fiscal year 2016 proposed budget includes Task Force Cyber Awakening—recommended investments amounting to $248 million for fiscal year 2016 and $721 million across the Future Years Defense Plan. Task Force Cyber Awakening will make additional recommendations on how to organize and resource capabilities to mitigate that risk.

Concomitant with the Task Force Cyber Awakening outcomes is the migration to a single defensible cyber architecture, which is vital to the continued success of Navy's worldwide operations. The Navy recognizes that the Joint Information Environment (JIE) is an operational imperative and endorses that vision, including the implementation of a single security architecture (SSA). The Department of the Navy intends for the Navy and Marine Corps Intranet (NMCI) to serve as the primary onramps into JIE, incorporating JIE technical standards through our network technical refreshment processes as those standards are defined. Through delivery of these enterprise environments, the Navy will achieve the tenets of JIE's framework of standards and architecture consistency.

For our part, U.S. Fleet Cyber Command is operationally focused on continuously improving the Navy's cyber security posture by reducing the network intrusion attack surface, implementing and operating layered defense in depth capabilities, and expanding the Navy's cyberspace situational awareness as outlined below.

REDUCING THE NETWORK INTRUSION ATTACK SURFACE

Opportunities for malicious actors to gain access to our networks come from a variety of sources such as known and zero day cyber security vulnerabilities, poor user behaviors, and supply chain anomalies with counterfeit devices from untrusted sources. Operationally, we think of these opportunities in terms of the network intrusion attack surface presented to malicious cyber actors. The greater the attack surface, the greater the risk to the Navy mission. The attack surface grows larger when security patches to known vulnerabilities are not rapidly deployed across our networks, systems, and applications. The attack surface also grows larger when network users, unaware of the ramifications of their on-line behavior exercise poor cyber hygiene and unwittingly succumb to spear phishing emails that link and download malicious software, or use peer-to-peer file sharing software that introduces malware to our networks, or simply plug their personal electronic device into a computer to recharge it.

The Navy is taking positive steps in each of these areas to reduce the network intrusion attack surface including enhanced cyber awareness training for all hands. Furthermore, we are bolstering our ability to manage cyber security risks in our networks through our certification and accreditation process, and through cyber security inspections across the Navy. Additionally, the Navy is reducing the attack surface with significant investments and consolidation of our ashore and afloat networks with modernization upgrades to the Next Generation Enterprise Network (NGEN) and the Consolidated Afloat Networks and Enterprise Services (CANES), respectively. Finally, the Navy is executing a Data Consolidation Center (DCC) strategy, which will reduce the number and variance of information systems at the same time allow for a centralized approach towards managing the confidentiality, integrity, and availability of our data.

For long-term success in cyber security, the Navy is working on improved acquisition and system sustainment processes. Specifically, we will design in resiliency by generating a common set of standards and protocols for programs to use as guiding principles during procurement, implementation, and the configuration of solutions, which will improve our cyber posture by driving down variance.

The Navy recognizes that all hands (users, operators, program managers, systems commands . . .) have an impact (for better or worse) on the magnitude of the Navy's attack surface and the mission risk associated with it. U.S. Fleet Cyber Command must defend this attack surface, regardless of size, using defense in depth capabilities described below.

DEFENSE IN DEPTH

The Navy is working closely with U.S. Cyber Command, NSA/CSS, our Cyber Service Partners, DISA, interagency partners, and commercial cyber security providers to enhance our cyber defensive capabilities through layered sensors and countermeasures from the interface with the public internet down to the individual computers that make up the Navy Networking Environment. We configure these defenses by leveraging all source intelligence and industry cyber security products combined with knowledge gained from analysis of our own network sensor data.

We are also piloting and deploying new sensor capabilities to improve our ability to detect adversary activity as early as possible. This includes increasing the diversity of sensors on our networks, moving beyond strictly signature-based capabilities (to include reputation-based and heuristic capabilities), and improving our ability to detect new and unknown malware.

JIE Joint Regional Security Stacks are also integral to our future defense in depth capabilities. As described above, the Navy has already consolidated our networks behind defensive sensors and countermeasures. We expect that JIE Joint Regional Security Stacks (JRSS) v2.0 will be the first increment to bring equal or greater capability to Navy Defense in Depth. Accordingly, the Department of Navy is planning to consolidate under JRSS 2.0 as part of the technical refresh cycle for NMCI when JRSS meets or exceeds existing Navy capabilities.

CYBER SITUATIONAL AWARENESS

Success in cyberspace requires vigilance: it requires that we constantly monitor and analyze Navy Networking Environment. We must understand both its availability and vulnerabilities. Furthermore we must be able to detect, analyze, report, and mitigate any suspicious or malicious activity in our networks. The Navy is planning to expand our current capabilities to include a more robust, globally populated and mission-tailorable cyber common operating picture. Additionally, with improved network sensor information across the DOD, however, comes the need for a single dedicated data strategy and big data analytics for all DOD network operations and defense data. This will allow for better overall situational awareness and improved speed of response to the most dangerous malicious activity by leveraging the power of big data analytics to harness existing knowledge rapidly.

U.S. FLEET CYBER COMMAND OPERATIONAL FORCES

U.S. Fleet Cyber Command's operational force comprises nearly 15,000 Active and Reserve sailors and civilians organized into 22 Active commands and 32 Reserve commands around the globe. The commands are operationally organized into a 10th Fleet-subordinate task force structure for execution of operational mission. Approximately 35 percent of U.S. Fleet Cyber Command 's operational forces are aligned with the cyber mission.

STATUS OF THE CYBER MISSION FORCE

As you may recall, during a hearing before the Senate Committee on Armed Services on March 12, 2013, General Keith Alexander briefed the Cyber Mission Force model, which DOD endorsed in December 2012. The Cyber Mission Force is designed to accomplish three primary missions: National Mission Teams will defend the Nation against national level threats, Combat Mission Teams to support combatant commander priorities and missions, and Cyber Protection Teams to defend Department of Defense information networks and improve network security.

Navy and other cyber Service components are building these teams for U.S. Cyber Command by manning, training, and certifying them to the U.S. Cyber Command standards. Navy teams are organized into existing U.S. Fleet Cyber Command operational commands at cryptologic centers, fleet concentration areas, and Fort Meade, depending upon their specific mission. Navy is responsible for sourcing four National Mission Teams, 8 Combat Mission Teams, and 20 Cyber Protection Teams as well as their supporting teams consisting of 3 National Support Teams and 5 Combat Support Teams.

The Navy is currently on track to have personnel assigned for all 40 Navy-sourced Cyber Mission Force Teams in 2016 with full operational capability in the following year. As of 1 March 2015, we had 22 teams at initial operating capability (IOC) and 2 teams at full operational capability (FOC). We are in the process of manning, training, and equipping our fiscal year 2015 teams to meet IOC standards by the end of fiscal year 2015. Additionally, between now and 2018, 298 cyber Reserve billets will also augment the Cyber Force manning plan as described below.

U.S. Fleet Cyber Command has also been designated as the Joint Force Headquarters-Cyber by U.S. Cyber Command to support U.S. Pacific Command and U.S. Southern Command in the development, oversight, planning and command and control of full spectrum cyberspace operations that are executed through attached Combat Mission and Support Teams. In 2014, Navy's Joint Force Headquarters-Cyber was certified and declared to have achieved full operational capability. This capability was attained without additional U.S. Fleet Cyber Command resources. As the Cyber Mission and Support Teams continue to grow and mature, additional resources to operationally control and manage these teams in support of combatant command priorities will be required.

RESERVE CYBER MISSION FORCES

Through ongoing mission analysis of the Navy Total Force Integration Strategy, we developed a Reserve Cyber Mission Force Integration Strategy that leverages our Reserve sailors' skill sets and expertise to maximize the Reserve component's support to the full spectrum of cyber mission areas. Within this strategy, the 298 Reserve billets, which are phasing into service from fiscal year 2015 through fiscal year 2018, will be individually aligned to Active Duty Cyber Mission Force teams and the Joint Force Headquarters-Cyber. Accordingly, the Joint Force Headquarters-Cyber and each Navy-sourced team will maximize its assigned Reserve sailors' particular expertise and skill sets to augment each team's mission capabilities. As our Reserve Cyber Mission billets come online and are manned over the next few years, we will continue to assess our Reserve Cyber Mission Force Integration Strategy and adapt as necessary to develop and maintain an indispensably viable and sustainable Navy Reserve Force contribution to the Cyber Mission Force.

FUTURE CYBER WORKFORCE NEEDS

The Navy's operational need for a well-trained and motivated cyber workforce (active, Reserve and civilian) will continue to grow in the coming years as we build out the balance of Cyber Mission Force and as we refine our needs to holistically address the challenges being informed by Task Force Cyber Awakening. We will depend upon commands across the Navy to recruit, train, educate, retain and maintain this workforce including the Chief of Naval Personnel, Navy Recruiting Command, Naval Education and Training Command and Navy's Institutions of Higher Education (United States Naval Academy, Naval Postgraduate School, and Naval War College.) Additionally, the establishment of Navy Information Dominance Force (NAVIDFOR) in 2014 as a Type Commander will go a long way in generating readiness for cyber mission requirements. NAVIDFOR will work closely with the man, train, and equip organizations across the Navy to ensure that U.S. Fleet Cyber Command and other Information Dominance operational commands achieve proper readiness to meet mission requirements.

RECRUIT AND RETAIN

There are many young Americans with the skill sets we need who want to serve their country. I am very encouraged by the dedication and commitment I see entering our ranks. I am awed by their dedication and growing expertise every day. We must consistently recruit and retain this technically proficient group of diverse professionals for the cyber mission to sustain this momentum.

In fiscal year 2014, the Navy met officer and enlisted cyber accession goals, and is on track to meet accession goals in fiscal year 2015. Currently authorized special and incentive pays, such as the enlistment bonus, should provide adequate stimulus to continue achieving enlisted accession mission, but the Navy will continue to evaluate their effectiveness as the cyber mission grows.

Today, Navy Cyber Mission Force (CMF) enlisted ratings (CTI, CTN, CTR, IS, IT) are meeting retention goals. Sailors in the most critical skill sets within each of these ratings are eligible for Selective Reenlistment Bonus (SRB). SRB contributes significantly to retaining our most talented sailors, but we must closely monitor its effectiveness as the civilian job market continues to improve and the demand for cyber professionals increases.

Cyber-related officer communities are also meeting retention goals. While both Information Warfare (IW) and Information Professional (IP) communities experienced growth associated with increased cyber missions, we are retaining officers in these communities at 93 percent overall. Both IW and IP are effectively-managing growth through direct accessions, and through the lateral transfer process, thereby ensuring cyber-talented officers enter, and continue to serve.

With respect to the civilian workforce, we are aggressively hiring to our civilian authorizations consistent with our operational needs and fully supported by the Navy's priority to ensure health of the cyber workforce. We have also initiated a pilot internship program with a local university to recruit skilled civilian and military cyber workforce professionals. Navy will measure the success of this approach as a potential model to harness the Nation's emerging cyber talent.

As the economy continues to improve, we expect to see more challenges in recruiting and retaining our cyber workforce.

EDUCATE, TRAIN, MAINTAIN

To develop officers to succeed in the increasingly complex cyberspace environment, the U.S. Naval Academy offers introductory cyber courses for all freshman and juniors to baseline knowledge. Additionally, the U.S. Naval Academy began a Cyber Operations major in the fall of 2013. Furthermore, the Center for Cyber Security Studies harmonizes cyber efforts across the Naval Academy.

Our Naval Reserve Officer Training Corps' (NROTC) program maintains affiliations at 51 of the 180 National Security Agency Centers of Academic Excellence at colleges around the country. Qualified and selected graduates can commission as information warfare officers, information professional officers, or intelligence officers within the Information Dominance Corps.

For graduate-level education, the Naval Postgraduate School offers several outstanding graduate degree programs that directly underpin cyberspace operations and greatly contribute to the development of officers and select enlisted personnel who have already earned a Bachelor's Degree. These degree programs include Electrical and Computer Engineering, Computer Science, Cyber Systems Operations, Applied Mathematics, Operations Analysis, and Defense Analysis. Naval War College is incorporating cyber into its strategic and operational level war courses, at both intermediate and senior graduate-course levels. The College also integrates strategic cyber research into focused Information Operations/Cybersecurity courses, hosts a Center for Cyber Conflict Studies to support wider cyber integration across the College, and has placed special emphasis on Cyber in its war gaming role, including a whole-of-government Cyber war game under active consideration for this coming summer or fall.

With respect to training of the Cyber Mission Force, U.S. Cyber Command mandates Joint Cyberspace Training and Certification Standards, which encompass procedures, guidelines, and qualifications for individual and collective training. U.S. Cyber Command with the Service Cyber Components has identified the advanced training required to fulfill specialized work-roles in the Cyber Mission Force. Most of the training today is delivered by U.S. Cyber Command and the National Security Agency in a federated but integrated approach that utilizes existing schoolhouses and sharing of resources. The Navy is unified in efforts with the other Services to build Joint Cyber training capability, leveraging Joint training opportunities, and driving towards a common standard.

DECLINING BUDGETS

While the overall Navy budget has been impacted by financial constraints and sequestration, the Navy has done a good job in terms of minimizing the budgetary impact on U.S. Fleet Cyber Command and the capabilities it employs to conduct its operations. Should this circumstance change and future budgets decline, however, there will be an impact to the capability and capacity to conduct operations in cyberspace. The scope and magnitude of such impacts would be driven by the scope and magnitude of a budget decline.

It is, however, possible to speak in broad terms regarding the potential areas of impact. Operations in cyberspace are highly dependent on people—to a certain extent our people are part of the warfighting platform in cyberspace. Budgetary declines impacting our ability to attract and retain the numbers of people with the requisite skills and experience would negatively impact the Navy's ability to conduct operations in cyberspace. Additionally, declining budgets affecting the ability of the Navy to implement initiatives described above that reduce the network intrusion attack surface, enhance defense in depth and cyber situational awareness, or modernize/migrate to the Joint Information Environment greatly jeopardizes the Navy's ability to accomplish all missions, since all Navy mission accomplishment depends on having an available and secure network. Finally, reductions to procurement accounts, beyond cyber operations- or network-specific budgets, traditionally have delayed or slowed modernization of programs across the Navy. The unintended consequence of delayed modernization is delayed cyber vulnerability remediation in everything from business applications to weapon systems.

SUMMARY

Our success in the maritime domain and joint operational environment depends on our ability to maintain freedom of maneuver and deliver effects within cyberspace. To ensure operational success in the maritime and other warfighting domains, defense of Navy and DOD networks and information is essential and cannot be separated from the overall maritime operational level of war.

In order to continue to progress in cyberspace operations, we must have sufficient resources to ensure we close any identified cybersecurity gaps and provide our workforce with the right capabilities to maintain our warfighting advantage. We must be prepared—both technologically and with skilled operators, civilian and uniformed—and remain innovative. The threat in cyberspace will only continue to grow despite our budgetary challenges. U.S. Navy freedom of action in cyberspace is necessary for all missions that our Nation expects us to be capable of carrying out including winning wars, deterring aggression and maintaining freedom of the seas.

I thank you for this opportunity to share U.S. Navy and U.S. Fleet Cyber Command operations and initiatives in cyberspace.

Senator FISCHER. Thank you, Admiral.

General Cardon.

STATEMENT OF LIEUTENANT GENERAL EDWARD C. CARDON, USA, COMMANDER, U.S. ARMY CYBER COMMAND

General CARDON. Madam Chairwoman Fischer, members of the subcommittee, it's an honor to be here on behalf of Army Cyber Command and 2nd Army alongside my fellow joint commanders. I appreciate the work of this committee to protect the American people from emerging threats and to ensure our military has the capabilities needed to defend the Nation.

The Army's gained tremendous momentum, both with institution and operationalizing cyberspace, but much work remains. For the institution, we've created the Cyber Center of Excellence at Fort Gordon, Georgia, and Army Cyber Institute, at the United States Military Academy. In addition, the Army is establishing the necessary service frameworks for building cyber capabilities for the Army and, by extension, the joint force.

Operationally, we've made progress supporting both the Army and combatant commands. With respect to the Cyber Mission Force, we have 25 of the 41 teams on mission now, and expect to have all 41 teams on mission by the end of fiscal year 2016, as planned. However, we're employing these teams as they reach initial operating capability. The threat, vulnerabilities, and mission set demand this sense of urgency. We're also building a total Army force to include 21 additional Army Reserve and Army National Guard cyber protection teams.

We're going to need more people, beyond what is required for the Cyber Mission Force, to build out the support required to fully employ the Cyber Mission Force and to build cyber capabilities for all Army formations. To better manage our people, the Army created a Cyber Branch 17, and we're exploring the creation of a cyber career field for our civilian personnel. For training, we have essentially funded Joint Model for Individual Training. We're working to build the collective training capabilities and associated facilities within a joint construct. For equipping the forces, we're developing and refining the necessary framework to give us the agility needed in programming, resourcing, and acquisition for the infrastructure, platforms, and tools. For more defensible architecture and network, we're partnered with the Army Chief Information Officer, Defense Information Systems Agency, and the Air Force for an extensive network modernization effort. These are critical to the joint information environment and to the security, operation, and defense of our networks.

Our budget priorities include fielding the Cyber Mission Forces, growing our joint force headquarters cyber, developing a skilled cyber workforce, highlighting capabilities for that Cyber Mission Force, and restationing our headquarters. The Army's fiscal year 2016 requested cyberspace operations budget is $1.02 billion, and that includes $90 million for our Fort Gordon operational headquarters facility. We've made tremendous progress. With your support, we'll have the necessary program resources to continue this momentum. We cannot delay, for the struggle is on us now.

Thank you, and I'm happy to answer your questions.

[The prepared statement of General Cardon follows:]

Prepared Statement by LTG Edward C. Cardon, USA

INTRODUCTION

Chairman Fischer, Ranking Member Nelson, and members of the subcommittee, thank you for your support of our soldiers and civilians, our Army, and our efforts to operationalize cyberspace. It is an honor to address this subcommittee on behalf of the dedicated soldiers and Army Civilians of U.S. Army Cyber Command (ARCYBER) and Second Army who work every day supporting Joint and Army commanders defending the Nation in cyberspace.

Army Cyber Command and Second Army have gained tremendous momentum building the Army's cyberspace capabilities and capacity. While making significant strides over the past 2 years, continued progress requires persistent congressional support in three core areas: people, operations, and technology. Put differently, we require resources, appropriate authorities, organizations, and capabilities, which can be synchronized in time and space with singular purpose to accomplish directed missions. This testimony focuses on the actions and activities the Army has underway, or is planning, to support our title 10 responsibilities to organize, man, train, and equip Army cyber forces for cyberspace operations.

MISSION AND ORGANIZATION

Army Cyber Command and Second Army directs and conducts cyberspace operations as authorized, or directed, to ensure freedom of action in and through cyberspace, and to deny the same to our adversaries. To accomplish this mission, the Secretary of the Army and the Army Chief of Staff streamlined the Army's cyberspace command and control structures by placing operational control of all Army operational cyber forces under one commander. The ARCYBER commanding general is responsible for Army and joint cyberspace operations; is designated as the Second Army commanding general responsible for all Army network operations (to meet United States Code titles 40 and 44 requirements as defined by Headquarters, Department of the Army); and is designated as the Army's Joint Force Headquarters-Cyber (JFHQ-Cyber) commander responsible for cyberspace operations supporting select geographic combatant commands as directed by U.S. Cyber Command (CYBERCOM). This construct enables unity of effort for cyberspace operations. The Secretary of Defense's recent decision to establish Joint Force Headquarters-Department of Defense Information Networks (DODIN) better aligns DODIN operations, and by extension, Army networks, in a joint construct. This decision is essential to realizing the Department's goal of establishing one joint global network that the Services operate within and extend for operational missions.

Other recent Army decisions include the formation of the Army Cyber Institute at the U.S. Military Academy, West Point, the establishment of the U.S. Army Cyber Center of Excellence (Cyber CoE) at Fort Gordon, GA, and the transition of the proponent for cyberspace operations from ARCYBER to the Army's Training and Doctrine Command at the Cyber CoE. The Cyber CoE is now the Army's center of gravity for institutionalizing cyberspace, to include developing the necessary doctrinal, organizational, training, and materiel activities and policies. We have already established the initial elements of Army JFHQ-Cyber at Fort Gordon, GA, and will collocate the ARCYBER headquarters alongside National Security Agency-Georgia at Fort Gordon by 2020. The fiscal year 2016 President's budget includes a request for $90 million to build a state-of-the-art headquarters and operations facility at Fort Gordon for Army Cyber Command.

To carry out our mission, ARCYBER and Second Army's budget priorities include fielding the Cyber Mission Forces; growing the Army's JFHQ-Cyber; developing a highly-skilled cyber workforce; piloting capabilities for Cyber Mission Forces; and restationing ARCYBER headquarters.

The budget for ARCYBER funds the headquarters activities supporting all Army cyberspace operations, including the Army JFHQ–Cyber and the Army Cyberspace Operations Integration Center. Information technology capabilities we are focusing on include network modernization, cyber analytics, network mapping, cloud and virtualization, and advanced platforms and tools. Additionally, we are working with the Army CIO/G–6 and acquisition community to strengthen cybersecurity across the Army.

BOUNDING THE IMPACT OF CYBERSPACE ON MILITARY OPERATIONS

Our momentum in cyberspace is also being driven by broader institutional changes to Army concepts. The Army's doctrine, Unified Land Operations, and recently published Army Operating Concept, establish a set of assumptions about conditions of the network and cyber-electromagnetic environment in which our forces are expected to operate. Services and combatant commanders base their plans on the expected Army capabilities, derived from this doctrine. Despite downsizing, the Army is adding capabilities that amplify military effects while allowing more effective operations in and through cyberspace. Commanders at all levels are synchronizing cyberspace operations into traditional land, sea, air, and space activities in time and space. They are simultaneously organizing networked assets, the electromagnetic spectrum, and kinetic forces in all domains to achieve a disproportionate advantage. Achieving operational success hinges on having the requisite command and control, alignment of authorities with missions, and other key enabling capabilities such as intelligence, targeting information technology and communication activities. Tactical and enterprise networks are converging and future networks and the data they carry will be more contested and challenged—especially in more intense forms of conflict.

Today the network is a critical enabler and also an operational capability for cyberspace operations. Army Cyber Command is charged to plan and direct cyberspace operations supporting both the Army and CYBERCOM, and these missions require unity of effort and unity of command.

Now that cybersecurity has to be considered an element of cyberspace operations, where does cybersecurity fit, within the DOD's full-spectrum of cyberspace operations? In other words, where does statutory responsibility for cybersecurity nest with the operational commanders' responsibility to conduct full-spectrum cyberspace operations?

To fully operationalize cyberspace, Army leaders and cyber organizations must be capable of ensuring both freedom of maneuver in cyberspace, and integrating interactions between cyberspace operations and our traditional military activities, that are increasingly reliant on networks and network-dependent enablers. This requires an agile and adaptive network that does not exist in the Army today. The Army recognizes it must collapse its vast array of disparate networks, enclaves, and nodes at both tactical and enterprise levels to improve security, effectiveness and efficiency through network modernization. In his recent House Armed Services subcommittee on Emerging Threats and Capabilities testimony, the Army's Chief Information Officer, LTG Robert Ferrell, described how the Army is achieving this modernization as part of the Joint Information Environment (JIE).

RECRUITING, RETAINING, AND DEVELOPING CYBERSPACE OPERATIONS PERSONNEL

The Army's first priority for cyberspace capabilities is to grow the Cyber Mission Force (CMF). We have increased our CMF capacity exponentially since September 2013 with 25 of 41 teams at initial operating capability. We are on track to have all 41 Army CMF teams established and operating by the end of fiscal year 2016. However, they will not all be fully operationally capable until fiscal year 2017.

Nothing is more important and vital to the growth of cyber capabilities than our ability to attract and retain the best people. As such, the Army views people as the centerpiece to cyberspace characterized by high degrees of competence and character. After a detailed study, the Army determined it needs 3,806 military and civilian personnel with core cyber skills. To help meet our personnel needs, the Secretary of the Army established a cyber branch on September 1, 2014, and discussions are ongoing to determine how to better manage civilians supporting cyberspace operations. In addition, the Army has also created an "E4" additional skill identifier to better track personnel who have served in cyber and cyber related assignments as we build the branch and the force.

The Army has enjoyed success with in-Service recruiting into the growing cyber force, and is actively working to expand access to high-quality recruits. We have increased recruiting aptitude scores, visibly expanded our marketing efforts, and started work on a Cyber CoE-led initiative to encourage Science Technology Engineering and Mathematics cadets from both U.S. Military Academy (USMA) and the Reserve Officers' Training Corps (ROTC). We will commission the first 30 cyber branch officers from both USMA and ROTC programs this summer. Once assessed into the cyber branch, officers are managed by the U.S. Army Human Resources Command's Cyber Management Branch.

Furthermore, the Cyber CoE, in collaboration with ARCYBER and other stakeholders is working to implement a cyber Career Management Field for enlisted personnel that will encompass accessions, career management, and retention this fiscal year. The Army recently approved Special Duty Assignment Pay, Assignment Incentive Pay, and bonuses for soldiers serving in operational cyber assignments. We have also expanded cyber educational programs, including training with industry, fellowships, civilian graduate education, and utilization of inter-service education programs (e.g., Air Force Institute of Technology and the Naval Postgraduate School). We are confident these will serve as additional incentives to retain the best personnel for this highly technical field.

Additionally, as part of our Total Force efforts, we have worked with the Reserve components on key retention initiatives, including bonuses for critical skill servicemembers transitioning from active duty service into the Reserve components; and accession bonuses for commissioned and warrant officers upon award of their duty qualifying military occupational specialties. Appropriate Special Duty and Assignment Incentive Pays should be considered for each of the Reserve components' cyber soldiers.

Recruiting and retaining Army civilian cyber talent is challenging, given internal Federal employment constraints regarding compensation and a comparatively slow hiring process. Current efforts to attract and retain top civilian talent include extensive marketing efforts, and leveraging existing programs and initiatives run by the National Security Agency, Office of Personnel Management, and National Science Foundation.

The targeted and enhanced use of recruiting, relocation, and retention bonuses, and repayment of student loans will improve efforts to attract, develop, and retain an effective cyber civilian workforce. These authorities exist but require consistent and predictable long-term funding. Retaining highly-skilled cyber professionals will continue to be a significant challenge that needs to be addressed.

TRAINING

Training is critical to building and retaining our cyberspace force. Individual and collective cyber training has four components: training the CMF; integration of cyber into unified land operations at echelon; training other cyber forces and enablers; and training to achieve basic cybersecurity awareness across the Total Army.

To fund CMF joint training requirements for Active component soldiers and civilians, the Department of Defense provided resources through CYBERCOM for all the Services through fiscal year 2016. This training allotment was only for Active component soldiers and civilians. Training and sustainment resourcing after fiscal year 2016 will become a Service responsibility, which the Army must fund beginning in 2017. To determine the way ahead for the transition to Service responsibility, the Army Cyber CoE recently conducted a Joint Cyber Training Forum with CYBERCOM and representatives from other Services and agencies. The forum concluded that the Services are best positioned to develop common core individual training for specific CMF work roles. Consequently, the Army is re-evaluating cyber-related training at its specialty schools to better align the curriculum with CMF requirements. To meet the growing demands for trained cyberspace operations personnel, and in accordance with the Total Army policy with reference to cyberspace, the Cyber CoE has initiated a partnership with the Army National Guard Professional Education Center in Little Rock, AR, to increase cyber training throughput.

Both ARCYBER and the Cyber CoE are developing robust collective training methods that include both simulated, virtual, and real-world operational events on ranges and networks that stress individual and team capabilities. We now require dedicated training facilities, support infrastructure and cyberspace live fire facilities consistent with joint range requirements at the Service and joint levels. Permanent training environments with dedicated facilities and resources will enable training innovations and further growth in capability and capacity available to combatant and Army commanders.

To help integrate cyberspace operations into unified land operations at echelon, Army Cyber Command works closely with Army Training and Doctrine Command to ensure the continuum of cyberspace leader development, education, and training remains current and relevant despite the high rates of technological change. The Cyber CoE is explicitly charged with incorporating joint standards into existing programs of instruction in Military Occupational Specialty schools and the Army Combined Arms Center is incorporating cyber operations planning into their training scenarios. The Army must place equal attention toward the training of our cyber network defense service providers, our computer emergency response teams, and our information technology professionals. Finally, the Army must continue to improve the effectiveness of cybersecurity training across the Total Army. This also requires a culture change.

The Army maximizes its contribution to the joint environment through fully participating in the design and conduct of CYBERCOM-sponsored and executed training and exercise events. Army Cyber Command has also incorporated cyberspace operations into multiple operational plans and major exercises—building a cadre of cyberspace planners now supporting the joint force and Army commanders. The Army recognizes that cyber capabilities should also extend and be executed at the tactical edge to provide our forces a winning advantage across warfighting functions; therefore, the Army is working hard to define cyber requirements, including training requirements, for cyber support to our Corps and below formations with pilot programs planned for this year. We continue to expand our professional cyberspace opposing force, to more effectively train organizations and individuals on how to better protect and defend themselves against cyber-attacks and how to operate in a degraded cyberspace environment during operational training events, such as major exercises and training center rotations.

RESERVE COMPONENTS INTEGRATION

Army Cyber Command is a total multi-component force of Active and Reserve components which are fully integrated into the cyberspace force mix. Building the U.S. Army Reserve (USAR) and Army National Guard (ARNG) cyber forces is a high priority for the Army and ARCYBER. Our Reserve Components integration strategy was reflected in the Army's input to the Department's response to section 933 of the National Defense Authorization Act for Fiscal Year 2014, titled "Cyber Mission Analysis for Cyber Operations of the Department of Defense," which requested an analysis of the Reserve components' role in cyberspace operations and is focused along several lines of effort, including: building an operational reserve in the USAR and ARNG for cyberspace crisis response; seeking opportunities to provide dual-use capability in support of Military and Homeland Defense and Defense Support of Civil Authorities missions; organizing cyber units to match CMF structure; aligning ARNG and USAR cyber forces under ARCYBER training and readiness authority; leveraging industry connected skills; and using the Reserve components' retention advantages for the Total Force.

The Army and ARCYBER will continue to develop a total multi-component Army cyber force that includes 21 Reserve Component Cyber Protection Teams trained to the same standards as the active Component cyber force. The civilian acquired skills and experience of Reserve component soldiers should be leveraged to provide equivalency for cyber training, enabling faster integration of the Reserve components' capability into the cyberspace force mix. In October 2014, in coordination with the Director of the Army National Guard, the Army activated one Army National Guard Cyber Protection Team in a title 10 status supporting ARCYBER and Second Army.

Army Guard and Reserve Forces routinely augment our headquarters now for cyberspace operations even as we work to build additional capability and capacity in the Guard and Reserve. Our Reserve components' contributions include supporting Operation Enduring Freedom, current operations in Southwest Asia, the Defense Information Systems Agency, CYBERCOM, the standup of Army JFHQ-Cyber, and the defense of Army networks. As we move forward with the ARNG and USAR to build the Total Army cyber force, we will continue to train and integrate 429 ARNG and 469 USAR soldiers into the Army's cyberspace operations.

Authorities are a complex problem. The 933 report was an excellent start for defining the critical role our Reserve components play in cyberspace operations. While title 10 authorities are clear, Title 32 and State Active Duty status require the application of varied State constitutional, legislative, and executive authorities and coordination with state agencies and officials. While every State is different, there is merit in developing a common approach for authorities and capabilities to facilitate rapid and effective response in cyberspace.

EQUIPPING THE ARMY'S CYBERSPACE OPERATIONS FORCE

As cyberspace grows more complex, and increasingly contested with sophisticated threats able to exploit known and unknown vulnerabilities, cyberspace operations and cybersecurity have become exceptionally critical to national security. Sophisticated software, that almost anyone can operate, is readily available for altruistic or nefarious purposes. Aided by the proliferation of dual-use technologies, cyber actors of all types take advantage of the connectivity, openness, and relative anonymity of cyberspace, as illustrated by the recent attacks on Sony Pictures Entertainment and Anthem health insurance. Today electronic hardware and software are increasingly embedded in everything from vehicles to guided missiles, and are often integrated into systems which are difficult and costly to update or upgrade. New threats or vulnerabilities are identified with increasing speed and at widely ranging intervals making updates time-consuming. These factors present new vulnerabilities and pose new threats to our warfighting systems.

To combat the growing threats to our networks, we have to modernize and move to the Joint Information Environment (JIE) as quickly as possible to improve mission effectiveness, enhance security, and increase efficiency—an imperative to protecting the DODIN. In conjunction with our joint partners, the Army is aggressively improving its defensive posture beginning with architecture modernization efforts that reduce attack surface area, improve bandwidth and reliability, and fortify our long-standing but ever-critical perimeter and defense-in-depth capabilities. Notably, the Joint Regional Security Stack (JRSS) initiative, a component of the JIE, will consolidate and improve the security of currently disparate networks, and provide foundational elements for enhanced situational awareness.

Recent intrusions plainly underscore the extent to which DOD lacks sufficient situational awareness, putting operations and sensitive data at grave risk. With the proliferation of cyberspace capabilities globally, situational awareness depends upon analysis of unprecedented quantities of data gathered across friendly, enemy, and neutral cyberspace. Essential data elements, providing clues to cyber-attacks, often originate deep within adversary space, and span our entire defenses. All of these separate data sources must be captured, aggregated, and correlated in near real-time to discover ever-evolving and diverse threats, including insider threats.

To improve our situational awareness in cyberspace, we are aggressively pursuing foundational cyber analytics capabilities. Coupled with architecture modernization, our efforts align directly with JIE standards and its Single Security Architecture construct. In parallel, we are pursuing several advanced technologies to include network mapping, cloud and virtualization, and cyber infrastructure, platforms and tools, all of which are also fully integrated with CYBERCOM's Unified Platform initiative. Additionally, we are an active partner with Defense Advanced Research Projects Agency on its PLAN X cyberwarfare program, developing foundational platforms for the planning and execution of cyber operations.

Given the pace of technological change in cyberspace, we must also address distinct requirements, resourcing and acquisition processes for cyber technologies affecting the entire spectrum of research, development, testing, evaluation, fielding, and sustainment. Dynamic and agile institutional processes are crucial to building and maintaining our decisive technological advantage. Recent updates to policy instructions for the Joint Capabilities Integration and Development System and the Defense Acquisition System provide a foundation for requirements and acquisition governance and management. These policy updates are rooted in agility, flexibility, and accountability to rapidly deliver cyberspace capabilities. The Army is also establishing fiscal and governance structures for investments and appropriations for urgent requirements.

To keep pace with technology, we must also capitalize on the cumulative innovative power of industry, academia, and our National Laboratories to develop, test, and pilot promising technology and concepts. This requires a willingness to engage in iterative development and testing, where success is measured by rapidly validating assumptions, failing cheaply, early, and often. Where resources are liberated from non-performing programs and applied to those demonstrating promise; and where new or enhanced cyberspace capabilities are delivered in weeks or months instead of months or years.

In recognition of the unique demands of cyberspace technologies, the Army has designated a cyber-focal point at the office of the Assistant Secretary of the Army for Acquisition, Logistics, and Technology, and designated initial cyber materiel development roles across our Program Executive Offices. The Army is deeply focused on improving the security posture and resilience of its critical weapons and business platforms, ensuring cyber threats and vulnerabilities are considered both in the design phase and throughout production and sustainment. In addition, the Army is focused on ensuring the advanced cyber technologies being procured for cyber mission forces today are integrated into comprehensive, sustainable acquisition programs that fully address defensive, offensive and DODIN cyberspace operations requirements. Remaining focused on DOD and CYBERCOM guidance and directives, we will ensure Army capabilities are presented in alignment with joint requirements and are interoperable within the joint community, optimizing our collective investments across DOD. As we work to ensure current processes evolve to capitalize on innovative technologies, ultimately, new programming and acquisition authorities would provide greater flexibility to developing and fielding the infrastructure, platforms, and tools needed by our operational cyber forces.

CONCLUSION

Operationalizing cyberspace is a journey. Army Cyber Command, Second Army, and Army JFHQ-Cyber have made tremendous progress operationalizing cyberspace for the Army. Army networks are better defended and our cyber forces are better manned, trained and equipped. Recent institutional changes are helping recruit, retain, and continuously develop competent and disciplined cyber professionals.

Despite cyberspace operations' central role in current defense strategy, today funding for core requirements remains uncertain. Cyber professionals—resourced with the right infrastructure, platforms and tools—are the key to dominance in cyberspace. Continued persistent congressional support is essential to ensure our Army has the required resources and authorities, and the right people, processes, and technologies to provide our combatant commanders and national decision makers with a ready, capable, and superior operational cyber force.

With your support, the Army will continue to provide national leaders and military commanders with an expanded set of options supporting national security objectives. With your support, we will deliver.

Senator FISCHER. Thank you, sir.

Thank you all for your service to this country, and thank you for being here today to answer our questions and provide us with some good information.

Admiral Tighe and General Wilson, I know that, both the Navy and the Air Force, you've established task forces to review weapon systems for vulnerabilities. And, as we're looking at those systems, I know that you want to ensure that they haven't been compromised, and also that they are configured to resist a cyber attack in the future. Can you tell us how you're prioritizing those reviews? And when do you expect to have those high-priority systems assessed?

Admiral TIGHE. Yes, Madam Chairman, I'll take the first shot.

From the Navy perspective, my command has been operationally involved in demonstrations to help us assess how at risk that the Navy missions may be. Beyond the responsibilities we have for our corporate networks, for our communications, for our C4ISR capabilities, we know that there are potential risks that exist inside of our weapon systems and inside of our control systems in our platforms. And so, our demonstration has helped to inform Navy investment decision-making from a Task Force Cyber Awakening, is the organization that was stood up by the CNO and by the assistant Secretary of the Navy for Research, Development, and Acquisition, to take a holistic view across all of the Navy investment portfolios, all of the Navy system commands and programs so that we are accounting for cyber security in the most holistic way in all of those programs.

Senator FISCHER. So, you're looking to see if anything's been corrupted within an existing system?

Admiral TIGHE. We're looking to make sure that cyber security is accounted for in every program that we are—you know, at developing and delivering to the Navy, every capability that may depend upon an operating system or something related to network in that regard. And so, Task Force Cyber Awakening has broken into three different subgroups to look—organizationally, do we have the right authorities to, again, go beyond the authorities that we execute, you know, in behalf—on behalf of cyber and communication systems and our networks, go into control systems, go into operating systems.

And, as it pertains to dealing with any vulnerabilities that may exist there, what is the right resource investment strategy to mitigate the risk that exists today, especially on our ships that we will have with us for many years to come? How will we mitigate any risk that may exist there? And how will we build the types of teams that we are building, aimed at communications and networks, for those types of systems, which are different skills, different tool sets, when you get into the realm of the combat systems and the——

Senator FISCHER. Right.

Admiral TIGHE.—and the control systems. And so, that's what——

Senator FISCHER. When do you expect that to be assessed, then?

Admiral TIGHE. We're expecting the Task Force Cyber Awakening to——

Senator FISCHER. I know the Navy's further along.

Admiral TIGHE. We are. It started in September. We are trying to get to completion on Task Force Cyber Awakening by this summer. But, there will be enduring resource investments, organizational changes, and potentially additional processes put in place, much like the SUBSAFE Program took on making sure water doesn't get into our submarines, thinking in terms of CYBERSAFE for our systems that go beyond the things that we are protecting and defending today.

So, by the summer, we should have a good feel for what are our next steps, whether we will be, you know, totally complete at that point. there's—there may be more work to be done, certainly more investment to be made, in terms of mitigating the risks that we are carrying.

Senator FISCHER. Okay. I just have a half-minute left.

Admiral TIGHE. Sorry.

Senator FISCHER. If I could have the other gentlemen—what's happening with the Air Force, and then the Marines and the Army, as well, on this?

General WILSON. Absolutely, ma'am. So, we—

Senator FISCHER. You have, like, a half—three of you, half-minute.

[Laughter.]

General WILSON. Ours is called Cyber Secure Task Force. The Chief and the Secretary just approved that, then it kicked off about a month ago—4 to 6 weeks ago. They've given us 12 months. It's a whole-of-Air-Force-effort initiative to look across programs, networks, as well as installations. It's focused on our core missions—air superiority, space superiority, global strike, command and control, *et cetera.* I think we've done a nice job in the network side, with some of the Cyber Mission Force standing up. There's a recognition that we may be vulnerable in our program of record. And so, that's really the focus. I mean, we're involved from the 24th Air Force perspective, but it's really a whole-of-service—CIO, program offices, PEOs, *et cetera.*

Senator FISCHER. Okay. Thank you.

General O'DONOHUE. The Marines are tracking with the Navy. We're part of Task Force Cyber Awakening. We have programs that we share with the other Services. We'll work with them as we go, comprehensively. And then, lastly, we're working with our acquisition community to get this at the root requirement as we get new systems coming in.

Senator FISCHER. Thank you, sir.

General.

General CARDON. And, ma'am, the Army, same as the others, specifically for the programs of record, given the scale of the Army's equipment, going forward, making cyber security a key performance parameter on all contracts, and then to work backwards, and then—over time. And then, finally, I would say this is a competitive space, so we're never really going to be done in this space. This is going to have to be something that we just constantly assess on a regular basis——

Senator FISCHER. General, have you budgeted for that?

General O'DONOHUE. It's not inside my budget. It's—would be inside the acquisition budgets. The Army's been having a—quite a debate about how much do we really fix, against which threats? And General Williamson and I are were—are working together on that, both of them.

Senator FISCHER. Thank you, sir.

Senator Gillibrand.

Senator GILLIBRAND. Thank you, Madam Chairwoman.

I appreciate all your presentations. And I was very excited to hear about a lot of the work you're doing to get the best cyber warriors you can. I think it's very exciting.

So, I want to look a little bit into the issue of the Reserve component, which you all mentioned, how you're addressing it. My understanding for the Air Force, that they plan to staff its Cyber Command requirements, in part, from the National Guard units. With regard to Army, do you also intend to staff part from National Guard units for your CYBERCOM requirements? And, if not, how do you plan to use the Reserve components, specifically?

General CARDON. So, ma'am, we have, in the Army National Guard, 1,035. They work in Cyber Command, in DISA, in my own headquarters, in the Joint Force Headquarters. And, of that, there are 11 Cyber Protection Teams. And one of those is on Active Duty now, up in Maryland.

Senator GILLIBRAND. And how do you do their training? Do they get a different kind of training or the same kind of training?

General CARDON. We're still—we just started growing. The one we have, we've received—17 have received equivalency training, thus far.

Senator GILLIBRAND. Oh, that's good.

General CARDON. So, they have to——

Senator GILLIBRAND. Seventeen individuals?

General CARDON. Correct. They have to be trained to the same standard that's——

Senator GILLIBRAND. Yeah.

General CARDON. For the others, working with the institution, education systems, the PEC, down in Arkansas, to get that online with the Cyber Center of Excellence, which will give them equivalency training for the training, as well. So, they'll all be trained to the same standard.

Senator GILLIBRAND. That's excellent.

And, for Air Force, how do you plan to train the—your Reserve components?

General WILSON. Ma'am, the same—to the same standard. They go through the same schoolhouse, same curriculum, same standard.

Senator GILLIBRAND. They'll just do it over time? It'll take them longer, because there are only—or would you have them in a—

General WILSON. They come right through the same schoolhouse, side by side with Active Duty members, whether they're Guard, Reserve, or——

Senator GILLIBRAND. So, you might activate them for a certain amount of time to get the training? Like activate you for the 6 months to get the training, or whatever it is?

General WILSON. You're right, spot on, ma'am.

Senator GILLIBRAND. That makes great sense, actually. That's terrific.

Do you think the Services need additional resources for this training, for this additional capacity? And, if you do, I hope you request it.

General WILSON. So, ma'am, for the Air Force, we've already built that into the model.

Senator GILLIBRAND. Okay.

General WILSON. We've invested in our schoolhouses both at Goodfellow, Keesler, and at Hurlburt, the first two being intermediate—or initial training for intel and our cyber training, and then, at Hurlburt for our intermediate training. And so, all of those adds have been put in place. We're looking at the training model in the out years to make sure that we're comfortable with the size of the pipeline that we have today. But, that's already been accomplished. Matter of fact, the courses are up and running full steam right now.

Senator GILLIBRAND. That's great.

And this was mentioned in the previous panel, but retention obviously is something important if you're going to invest up to 2 years training these cyber warriors. Do you have plans on how to retain them, whether it's through, I don't know, compensation or—I don't know what plan you would—or approach you would take.

General WILSON. So, ma'am, in the Air Force, we have several different retention initiatives, both for Active and for Reserve and Guard. We like to say we'll never compete on price. We just are not going to be able to—

Senator GILLIBRAND. You certainly——

General WILSON.—compete on price.

Senator GILLIBRAND.—can't, yeah. [Laughter.]

General WILSON. It just isn't going to happen. So, we do look at targeted reenlistment bonuses. We look—we're considering proficiency pay for certain skill sets, when they achieve certain skills. To be honest, it's the pride of service, it's the fact that there's a pretty interesting mission set, and we empower and give a lot of responsibility for very young folks. We find they have a passion. Not everybody is going to stay in the Service. That's just a fact. The first thing we do when they think about getting out of the active Duty is, we put our arms around them and talk to them about the Guard and Reserve opportunities out there.

Senator GILLIBRAND. That's great, yeah.

General WILSON. And if that's not the case, that's okay. We consider it an investment for the country, and we'll restock the pipeline.

Senator GILLIBRAND. Can you update me a little bit on Rome Labs and how that's being developed?

General WILSON. I'm sorry, ma'am, didn't——

Senator GILLIBRAND. Can you update me on Rome Labs and how that's being developed for the Air Force?

General WILSON. Absolutely. So, ma'am, Rome Labs is key. It's one of our science and technology wheelhouses. It's the epicenter for our S&T work. It's a very tight relationship with regard to the technology that's come out of Rome Labs. We're taking a look at the portfolio and then how to accelerate some of the technologies that are coming out of the labs, and how do we field it, make it operational in a more rapid fashion. And so, that's—it's key to the partnership there.

Senator GILLIBRAND. Sure.

And, Lieutenant General, can you talk a little bit about how West Point's doing? I thought their cyber training was very impressive when I was last there. And I met a number of the cadets that were focused on that, and I thought it was really inspiring.

General CARDON. So, this year we'll assess 30 cadets into 17—15 from the Reserve Officer Training Programs, 15 from the Academy. The Academy has adjusted their programs to account for cyber security, so I think that is going to be a tremendous benefit here for the future.

Like with the Navy, they're—we're also exposing all of the officers to cyber security, because this has to become part of the foundational education that we expect them to have.

If I could just loop back on the retention really quick. On the high-end operators, what we've started doing is using 6-year enlistments. We're having no troubles filling that. The retention, I think, all of us are working through what is the best model to retain them.

Senator GILLIBRAND. And the other thing that I was impressed by at Fort Drum was that they're off the grid. And I thought that was vital, in terms of cyber defense and cyber missions, that there's an independence, where you can't be subverted or isolated because of energy needs. So, I would recommend to all the Services, to the extent we have assets anywhere around the world, that ability to be off the grid is vital, in terms of protecting infrastructure and protecting abilities to respond. So, thinking long-term, defensively.

Admiral TIGHE. I think the Navy, as part of Task Force Cyber Awakening and our shore infrastructure folks, recognize that we are dependent on a combination, obviously, of power generation that is internal to the Navy and commercial power providers, and then—you know, that extends to overseas in all the complexities there. So, our facilities folks have taken a—taken on a special project to go study and look at what is—what does "good" look like, in terms of the resiliency that we need to be resistant to any type of attack on that infrastructure upon which you depend.

Senator GILLIBRAND. Thank you.

Thank you all. Very grateful.

Senator FISCHER. Thank you, Senator.

Thank you all. I would invite you to join us in the SCIF for a classified briefing.

And, with that, I will adjourn the open hearing today.

Thank you.

[Whereupon, at 4:07 p.m., the subcommittee adjourned.]

[Questions for the record with answers supplied follow:]

QUESTIONS SUBMITTED BY SENATOR KELLY AYOTTE

IRAN'S RECENT CYBER ACTIVITIES

1. Senator AYOTTE. General McLaughlin, how would you describe Iran's cyber activities and capabilities generally?

General MCLAUGHLIN. [Deleted].

2. Senator AYOTTE. Mr. Rosenbach and General McLaughlin, has Iran conducted cyberattacks or cyber intrusions against the United States or our allies in the last year or so? To the degree you are able, please provide an unclassified response.

Mr. ROSENBACH. A growing number of computer forensic studies by industry experts strongly suggest that several nations—including Iran—have undertaken offensive cyber operations against private sector targets to support their economic and foreign policy objectives, at times concurrent with political crises. As DNI Clapper noted, Iranian actors have been implicated in the 2012–13 distributed denial of service attacks against U.S. financial institutions and in the February 2014 cyber attack on the Las Vegas Sands casino company.

General MCLAUGHLIN. Recent Iranian cyber operations likely include the destructive attack impacting Saudi Arabia's national oil company, Aramco, in 2012, and Iranian hackers penetrating the U.S. Navy and Marine Corps unclassified networks in 2013. Iranian hackers also harvested U.S. Government login and password information by fabricating an article from a security company "Newcaster" to redirect readers to an information gathering site.

More recently, the Director of National Intelligence testified before the Senate Armed Service Committee, on February 26, 2015, that Iran was responsible for a destructive cyber attack against a Las Vegas casino in February 2014. These attacks combined with continued distributed denial of service attacks targeting the U.S. financial sector show Iran's continued perseverance and cyber ambition.

LEVERAGING THE NATIONAL GUARD

3. Senator AYOTTE. General Cardon, Admiral Tighe, General Wilson, and General O'Donohue, given the expertise that resides in the Reserve component and the relative cost efficiency of the Reserve component, including the Guard, please provide more detail regarding how your Service is utilizing the Reserve component to improve and build your Service's cyber capabilities?

General CARDON. The Army and Army Cyber Command, as the Army's component to U.S. Cyber Command, continue to build a Total Army approach for our cyber forces that will provide staff augmentation and support to Joint and Army commands. Current examples of such Reserve component support include:

The Army Reserve Cyber Operations Group conducting Defensive Cyberspace Operations support and provides Department of Defense Information Network operations and Computer Network Defense Service Provider support to the Southwest Asia Cyber Center.

United States Army Reserve providing U.S. Cyber Command with cyberspace planners, an intelligence fusion cell, and joint personnel to man critical positions within the command.

The Virginia Army National Guard Data Processing Unit, conducting cyber operations in support of U.S. Cyber Command.

The United States Army Reserve Military Intelligence Readiness Command, which will transition to the Army Reserve Intelligence Support to Cyberspace Operations Element, providing intelligence support and analysis products to U.S. Cyber Command.

United States Army Reserve personnel also serve within the Army's Joint Force Headquarters-Cyber to execute joint cyberspace operations for U.S. Cyber Command.

The Army's plan includes one Army National Guard cyber protection team currently serving on active status, 10 Army National Guard cyber protection teams, and 10 United States Army Reserve cyber protection teams being built through Fiscal Year 2018 – all essential components of the Total Army cyber force. They will be trained to the same standard as the Cyber Mission Force.

The United States Army Reserve and Army National Guard are integral components of Army Cyber Command's Total Army approach to cyberspace operations.

Admiral TIGHE. The Navy takes pride in its ability to integrate its Reserve resources, under the Total Force Concept, in order to accomplish our various global missions. This is no different in the Cyber realm. We are utilizing our current inventory of highly skilled Reserve personnel to augment the Active Duty units assigned to defend, operate, and deliver effects through our networks. We are growing our capabilities in tandem with our Reserve Component by blending them into training, unit level certification events and joint exercises.

In addition, we are implementing a Reserve Cyber Mission Force (CMF) Integration Strategy, leveraging our Reserve Sailors' military and civilian expertise, which best postures the Navy to engage threats across the entire cyber mission set. In support of this strategy, there are 298 Reserve billets, which the Navy is phasing into service from FY15 through FY18 that will be aligned to Active Duty CMF teams and our Joint Force Headquarters-Cyber (JFHQ–C). This alignment strategy will allow Active Component CMF teams to capitalize on Reserve personnel's specific cyber-related skillsets and knowledge. Navy Reserve Sailors assigned to CMF billets provide operational support to the team's respective operational commander, including Fleet Commanders, U.S. Pacific Command, U.S. Southern Command, U.S. Cyber Command, and the Defense Information Systems Agency. As the Navy builds its Reserve CMF support structure, Fleet Cyber Command and TENTH Fleet will conduct assessments to maximize the Reserve Force's support to CMF operational objectives.

General WILSON. AFCYBER/24 AF/JFHQ–C is fully partnered with the Air Reserve Component (ARC) as part of its current and future build-up of cyber operations to support the Air Force's cyber mission and the DOD's Cyber Mission Force (CMF). They attend and meet the same training standards as our Active Duty operators.

From the outset, the ARC, in support of AFCYBER, has been integrated into the Cyber Mission Force build-up of 39 teams. To meet the demand signal of the CMF construct, the Air Force Reserve Command (AFRC) is standing up one Classic Associate Unit in FY16, integrating into a Regular Air Force Cyber Protection Team (CPT) squadron, providing steady-state capacity of one CPT or 30% day-to-day mission share. If mobilized, it will be able to provide manning for three CPTs in a surge capacity.

In addition to the team build in the CMF, the AFRC supports numerous other cyber missions under the 960th Cyberspace Operations Group (CyOG). The 960 CyOG is comprised of nine squadrons. These units defend Air Force Networks and key mission systems, train personnel, develop new weapon systems and tools, and provide command and control of cyber operations. In addition to the 960 CyOG, there are Individual Mobilization Augmentees (IMAs) under AFCYBER/24 AF/JFHQ–C that support various cyber missions.

Between FY16–FY18, the Air National Guard (ANG) is building 12 unit-equipped squadrons to sustain two steady-state CPTs, with each organized into the 30/70 full-time/part-time ratio. The ANG is also standing up a National Mission Team unit in FY16. These units will align under two ANG Cyberspace Operations Groups.

In addition to the build-up within the CMF Teams, the ANG support to cyber operations includes five cyber units. These units support defensive cyber operations and command & control. Additionally, the Air Guard has one of only three of the Network Operations Squadrons in the Air Force.

Finally, the ARC plays a significant role in our engineering and installation and combat communications. There are 38 AFRC and ANG units supporting these missions and in the last two years the ARC deployed over 800 personnel supporting the warfighter with these capabilities.

General O'DONOHUE. For the Marine Corps, we currently provide reserve component augmentation to the MARFORCYBER headquarters and to the Marine Corps Network Operations and Support Center (MCNOSC). Informed by the Reserve Forces Policy Board report to Congress, "The Department of Defense Cyber Approach: Use of the National Guard and Reserve in the Cyber Mission Force" and with guidance from the Commandant, we have begun the process to expand the role of the Marine Corps Reserve at MARFORCYBER. The increased role of the reserve will build a surge capacity for times of crisis, and capture the unique skills of Reserve Marines with civilian cyber skills. As suggested by the report, we will review our strategy in FY17.

CYBER AS ITS OWN SERVICE BRANCH

4. Senator AYOTTE. Mr. Rosenbach, Secretary Carter recently suggested that "there may come a time" when the cyber corps may become its own Service branch. Instead of each Service developing redundant capabilities at great expense, would it make more sense to have a consolidated cyber corps as its own Service?

Mr. ROSENBACH. As the Secretary said, there may come a time when a cyber corps may warrant its own Service branch, but that time is not now. Much like each Service has a Special Forces community that embeds under USSOCOM, today each Service organizes, trains, and equips the Cyber Mission Force under USCYBERCOM. Since each Service has unique cyber requirements, they are each organized a little differently, bringing Service personnel with a variety of backgrounds, including the military intelligence, Signals Intelligence, cyber operations, information assurance, and information technology career fields, to make up the cyber force. Additionally, last year, the Department developed a Total Force strategy that would integrate approximately 2,000 Reserve Component personnel into the workforce as well. This strategy ensures that DOD embraces cyber expertise from all sources integrating diversity of thought, capabilities, experiences, rapid innovation, and best practices. The current strategy provides flexibility to address both Cyber Mission Force and Service-specific cyber needs and readiness. Additionally, since all forces are trained and equipped to the same joint standard, it is unlikely there would be resource efficiencies in creating a new Service Branch at this time.

5. Senator AYOTTE. General O'Donohue, Secretary Carter recently suggested that "there may come a time" when cyber corps may become its own Service branch. Why does the Marine Corps need an organic cyber capability?

General O'DONOHUE. An organic cyberspace capability allows the Marine Corps to integrate cyberspace considerations into military operations in line with our unique role in the joint force as the Nation's expeditionary force in readiness. The Marine Corps' maneuver warfare and combined arms doctrine relies on integration of all warfighting capabilities in one organization - the Marine Air-Ground Task Force (MAGTF). Separating organic cyberspace capabilities from the Marine Corps, and centralizing them into their own service, would limit the MAGTF Commander's ability to integrate cyberspace considerations into military operations and mitigate risk to their missions.

However, the Marine Corps and the MAGTF is designed to be part of a broader Joint Force. We expect our Joint, interagency and coalition partners to compliment our cyberspace operations through information sharing, development of capabilities, and operational coordination. Likewise, as we integrate cyber capabilities into the MAGTF and the Marine Corps as a service, we expect to expand our role of providing cyber capabilities to the joint force through our commitment to USCYBERCOM.

6. Senator AYOTTE. General O'Donohue, why shouldn't we use the Marine Corps' end strength numbers to support expeditionary operations and leave cyber to a separate cyber corps?

General O'DONOHUE. Cyberspace impacts every aspect of a 21st century expeditionary operation. Marines forces must be knowledgeable and sophisticated in cyberspace operations in order to conduct one of their most essential tasks—the ability to command and control subordinate units across the battlefield. Dedicating a portion of our end-strength to the mastery of cyberspace operations is essential to properly resourcing operational Commanders to conduct effective command and control, validate threats, and assess risks. Whether or not a separate cyber corps is established, Marines must be proficient in cyberspace to effectively operate.

7. Senator AYOTTE. General O'Donohue, are there challenges specific to Marine Corps cyber operations that other branches do not face?

General O'DONOHUE. All branches face challenges and threats in cyberspace. The Marine Corps' role as our nation's expeditionary force in readiness requires additional flexibility. Providing a comprehensive crisis response force that utilizes and operates effectively across all domains presents unique challenges and opportunities to our Marine Air Ground Task Forces (MAGTFs). The Marine Corps is undergoing a fundamental transformation to adapt to those unique challenges and opportunities in the cyberspace domain. As we undergo this transformation, we will maintain our unique service character and warfighting ethos, but we will not be bound by the past. Our Commandant has laid out a clear vision to reset our network on warfighting principles and integrate cyberspace operations into the Marine Air-Ground Task Force. In the coming years this will require the development of a cyberspace reserve component, a 'cradle-to-grave' lifecycle management process of our cyber workforce, and the integration and normalization of cyberspace into the MAGTF. We are addressing these unique challenges through an institutional focus led by Headquarters Marine Corps' "Task Force Cyber" and through collaboration with our industry partners and academia.

ATTRIBUTION CAPABILITIES

8. Senator AYOTTE. Mr. Rosenbach, General McLaughlin, General Cardon, Admiral Tighe, General Wilson, and General O'Donohue, on April 1st, the President declared a national emergency to deal with malicious foreign cyber activities, and authorized sanctions against anyone who uses cyber activities to threaten our national security, foreign policy, financial stability, or who steals trade secrets. However we cannot employ cyber countermeasures or impose sanctions that are critical to deter-

rence unless we can identify the attacker. To what degree are we able to attribute specific cyber-attacks to specific individuals?

Mr. ROSENBACH. Attribution has always been a challenge in cyberspace, but the Department has made significant progress in this area. Even the stealthiest cyber intruders leave footprints on victim networks and the infrastructure they misuse to conduct their activities. Those footprints grow more evident when those intruders are attempting to steal intellectual property on a massive scale from across the U.S. private sector or to penetrate large swathes of our critical infrastructure.

The Department, U.S. law enforcement, and the intelligence community have invested significant resources in collection, analysis, and synthesis of all-source intelligence to unmask malicious actors' cyber personae, identify the point of origin of their activity, and understand adversaries' tactics, techniques, and procedures. Over time, this allows us to identify with significant confidence groups of actors with common intent and broad campaigns of activity targeting specific sectors, and can reveal sufficient information to identify specific individuals.

The Department of Justice's May 2014 indictments of five members of the People's Liberation Army for cyber espionage against U.S. firms is an excellent example of how the U.S. Government is able to work together to attribute specific cyber activities to individuals. We would draw from the same tools and capabilities to enable attribution for the purpose of sanctions.

General MCLAUGHLIN. Our ability to determine attribution for cyber attacks depends on several factors including sophistication of the malicious actors, information sharing capabilities and policies, and available trained manpower. Attribution involves an examination of malicious activity based on technical, behavioral, and personal characteristics. Our ability to determine attribution does not solely rely on the mechanical process of geolocation of physical networks or nodes. The possibility always exists the adversary has exploited/hijacked what appears to be the origin and is directing the cyber attacks from a remote location, anywhere in the world.

Over the past decade, our ability to identify malicious cyber actors has improved significantly as we have adopted a federated approach in the analysis of data necessary to pinpoint the nexus for a given cyber operation. To stay ahead of the adversary, there are currently processes in place to share information and analytic insight across the DOD and the Intelligence Community. In addition, defense contractors and other civilian organizations have their own sets of information which assists in leading to the attribution of cyber threat actors and their capabilities and intentions.

General CARDON. We rely completely on the Intelligence Community for attribution of cyber threats. Our close relationship with the Army's G2 and INSCOM as well as relationships with the National Intelligence Community enable us to conduct more focused cyber operations. Expanding each military Service's Counter Intelligence cyber investigative and forensic capability and capacity would assist in providing attribution authorities more comprehensive data surrounding malicious cyberspace activity.

Admiral TIGHE. Service Components rely on the attribution authority and capability of NSA, USCYBERCOM, FBI and DHS to determine attribution of cyber activity as directed by ODNI. To assist with attribution capability, Service Cyber Components provide timely and accurate data of malicious activity on Service networks. Increasing network sensors and detection systems would assist Service Components in providing timely and accurate data to the responsible attribution authority. Additionally, expanding each military Service's Counter Intelligence cyber investigative and forensic capability and capacity would assist in providing attribution authorities more comprehensive data surrounding malicious cyberspace activity.

General WILSON. Our ability to determine attribution for cyber attacks depends on several factors including sophistication of the malicious actors, information sharing capabilities and policies, and available trained manpower. Attribution involves an examination of malicious activity based on technical, behavioral, and personal characteristics. Our ability to determine attribution does not solely rely on the mechanical process of geolocation of physical networks or nodes. The possibility always exists that an adversary has exploited/hijacked from what appears to be the origin, but is directing the cyber attacks from a remote location, anywhere in the world.

Over the past decade, our ability to identify malicious cyber actors has improved significantly as we have adopted a federated approach in the analysis of data necessary to pinpoint the nexus for a given cyber operation. To stay ahead of the adversary, there are currently processes in place to share information and analytic insight across the DOD and the Intelligence Community. In addition, defense contractors and other civilian organizations have their own sets of information which assist in leading to the attribution of cyber threat actors and their capabilities and intentions.

General O'DONOHUE. As outlined in the forthcoming DOD Cyber Strategy 2015, attribution is a fundamental part of an effective cyber deterrence strategy as anonymity enables malicious cyber activity by state and non-state groups. In coordination with U.S. Cyber Command, our ability to determine attribution for cyber attacks is impacted by several factors including the sophistication of the malicious actors, our information sharing capabilities and policies, and the depth and capacity of our cyber workforce. Our ability to determine attribution relies on the examination and assessment of the malicious activity based on technical, behavioral, and personal characteristics. While it is certainly difficult to definitively attribute malicious cyberspace actions, the cyberspace community has developed and implemented robust methodologies that begin with the malicious event and take into account all applicable aspects to include the victim of the attack, the infrastructure employed by the attacker, and the demonstrated capability of the attacker.

Our collective ability to identify malicious cyber actors has improved significantly in recent years, as we have adopted the federated approach in the analysis of data necessary to pinpoint the nexus for a given cyber operation. To stay ahead of the adversary, there are currently processes in place to share information and analytic insight across the DOD and the Intelligence Community.

9. Senator AYOTTE. Mr. Rosenbach, General McLaughlin, General Cardon, Admiral Tighe, General Wilson, and General O'Donohue, what can we do to increase our attribution capabilities?

Mr. ROSENBACH. Attribution is a fundamental part of our cyber deterrence strategy as well as being critical to our ability to respond to a cyber attack in a timely and appropriate way. The Department, U.S. law enforcement, and the intelligence community have invested significant resources in collection, analysis, and synthesis of all-source intelligence to unmask malicious actors' cyber personae, identify the point of origin of their activity, and understand adversaries' tactics, techniques, and procedures.

DOD also collaborates closely with the U.S. private sector and other Federal departments and agencies to broaden our understanding of malicious activity, which improves our ability to attribute the origin of such activity as confidently and rapidly as possible. To that end, legislation that facilitates cyber information sharing between the U.S. Government and private sector will support the whole-of-nation approach that is necessary to protect against, prevent, detect, and respond to cyber threats..

Along with its intelligence community components, U.S. Cyber Command's National Mission Teams will be crucial to the Department's contribution to tracking foreign cyber adversaries in order to respond proactively to their evolving tactics, techniques, and procedures, as well as to changes in the focus of their malicious activities as they maneuver in cyberspace. This will be essential if we are to gain sufficient warning to be able to take action to prevent or respond to an impending attack of significant consequence. We appreciate Congress's support as we expedite the building of these National Mission Teams.

Finally, the counterintelligence organizations of the Military Departments are uniquely positioned to improve our insight into, and to frustrate and defeat, cyber espionage. The Military Departments and the Under Secretary of Defense for Intelligence, in consultation with the Principal Cyber Advisor, are developing a strategy that will specify how the military counterintelligence organizations will collaborate more effectively with the broader U.S intelligence and law enforcement communities on investigations and human and technical operations that thwart foreign cyber intelligence activities directed against the Department and the defense industrial base. We appreciate Congress's support as we appropriately resource these efforts.

General MCLAUGHLIN. As outlined in the recently released DOD Cyber Strategy, improving our ability to attribute malicious cyber activity is a cornerstone in protecting the nation's cyber enabled critical infrastructure.

Training, recruitment, and retention of effective information technology and analysis personnel are critical to building and maintaining an effective cyber force. Our current build-up of the Cyber Mission Force is a step in the right direction. It is also important we continue to strengthen the cyber ranks of existing agencies by hiring the most qualified individuals at all experience levels by providing working environments that are competitive with the private sector.

Substantial investment in research and development of new capabilities by private enterprise, educational institutions, and government agencies is also critical to improving our attribution capability. Attribution capability is highly dependent upon our mastery and dominance of communication and system technologies.

Finally, the sharing of malicious cyber activity and associated intelligence between the government and the private sector is key in the process of understanding the cyber adversary. As attribution models and frameworks continue to mature, unique insights and information can be shared and organized to deliver more rapid and accurate attribution. Combining private sector knowledge of threat streams on their systems with the government's knowledge of the same threat streams raises the collective understanding of adversary tactics, techniques, and procedures. This is consistent with the Administration's emphasis on the urgent need for cyber security legislation. Current legislative initiatives would create the necessary conditions for effective and efficient information sharing.

General CARDON. All attribution information received by Army cyber forces is received through a collaboration of DOD, DOJ(FBI), DHS, and other DOD and federal intelligence agency capabilities. Any legislation that would facilitate cyber information sharing between the U.S. Government and the private sector would more fully embrace a whole-of-nation approach by providing real time intelligence, and better equipping us to prevent, detect and respond to cyber threats.

Admiral TIGHE. Service Components rely on the attribution authority and capability of NSA, USCYBERCOM, FBI and DHS to determine attribution of cyber activity as directed by ODNI. To increase this attribution capability, Service Cyber Components provide timely and accurate data of malicious activity on Service networks. Expanding each Service's defense-in-depth approach to network sensor and detection system coverage, data retention capacity, and supporting analytics would assist Service Components in providing timely, accurate, and comprehensive data to the responsible attribution authority.

General WILSON. As outlined in current legislative initiatives and the recently released DOD Cyber Strategy, improving our ability to attribute malicious cyber activity is a cornerstone in protecting the nation's cyber enabled critical infrastructure.

Training, recruitment, and retention of effective information technology and analysis personnel are critical to building and maintaining an effective cyber force. Our current build-up of Cyber Mission Forces is a step in the right direction. It is also important we continue to strengthen the cyber ranks of existing agencies by hiring the most qualified individuals at all experience levels by providing working environments that are competitive with the private sector.

Substantial investment in research and development of new capabilities by private enterprise, educational institutions, and government agencies is also critical to improving our attribution capability. Attribution capability is highly dependent upon our mastery and dominance of communication and system technologies.

Finally, the sharing of malicious cyber activity and associated intelligence between Federal agencies and the private sector is key in the process of understanding the cyber adversary. As attribution models and frameworks continue to mature and are shared and agreed across agencies, each agency's unique insights and information can be shared and organized to deliver more rapid and accurate attribution. Combining commercial threat streams with the greater levels of signals intelligence, law enforcement/counterintelligence, and human intelligence collection, the Intelligence Community gains a better understanding of adversary tactics, techniques, and procedures.

General O'DONOHUE. As outlined in the forthcoming DOD Cyber Strategy 2015, the U.S. requires strong intelligence, forensics, and indications and warning capabilities to reduce anonymity and increase confidence in the attribution of malicious actors. Mastery and dominance of communication and system technologies are critical to the fidelity of these capabilities. In order to build and maintain this level of proficiency, we must recruit and retain the most qualified individuals. Through persistent training and collaboration with private enterprise, educational institutions, and government agencies, we must build the collective capacity of an effective Cyber Mission Force. Additionally, by leveraging the skills and capabilities of our allied partners, we can increase the potential to close gaps and achieve attribution of specific cyber-attacks to state or non-state actors.

Additionally, the sharing of malicious cyber activity and associated information between Federal agencies and the private sector is critical to understanding our cyber adversaries. As attribution models and frameworks mature, each agency's unique insights can be leveraged to deliver more rapid and accurate attribution. Commercial threat streams augment and enhance our level of understanding of adversary tactics, techniques, and procedures.

Question Submitted by Senator Jeanne Shaheen

DOD AND DHS CYBER COLLABORATION

10. Senator SHAHEEN. Mr. Rosenbach and General McLaughlin, can you describe the Department of Defense's (DOD) efforts to collaborate and share information with the Department of Homeland Security (DHS) in terms of planning, operational structure, and efforts to address external threats?

Mr. ROSENBACH. DOD works very closely with its interagency partners to ensure that it is building and implementing a whole-of-government approach to cybersecurity. DOD's relationships with DHS and the Department of Justice (DOJ) are and must remain strong, as DHS and DOJ have the lead for domestic response to cyber threats. In this context, DOD has a more limited support role.

DOD and DHS regularly collaborate and share information through a variety of channels, ranging from daily communication between operational centers to interagency forums such as the Cyber Response Group and Unified Coordination Group. The two organizations also exercise together to ensure unity of effort across the departments.

In 2010, the Secretaries of Defense and Homeland Security signed a Memorandum of Agreement (MOA) for sharing personnel, equipment, and facilities in order to increase interdepartmental collaboration, mutual support for cybersecurity capabilities development, and synchronization of current operational cyber mission activities. Today, we are developing ways to improve collaboration and information sharing to protect and defend U.S. critical infrastructure, to create consistent approaches to cybersecurity across both national security and non-national security systems, and to enhance our ability to prevent, mitigate, respond to, and recover from domestic cybersecurity incidents.

General MCLAUGHLIN. The Department of Defense (DOD) and the United States Cyber Command (USCYBERCOM) maintain a healthy, positive, and productive collaboration and information sharing relationship with the Department of Homeland Security (DHS), focused within the National Protection and Programs Directorate (NPPD) Office of Cyberspace and Communications (CS&C). The terms of this relationship are set forth in the 2010 Memorandum of Agreement (MOA) between DHS and the DOD regarding Cybersecurity, and are further described in the 2013 U.S. Federal Cybersecurity Operations Team National Roles and Responsibilities chart and other applicable vision statements and strategy papers.

Routine collaboration and information sharing between USCYBERCOM and DHS revolves around the daily interaction between the USCYBERCOM Joint Operations Center (JOC) and the DHS National Cybersecurity and Communications Integration Center (NCCIC), as well as the physical presence of exchanged liaison officers within those cyber centers. The JOC and the NCCIC participate in twice daily operational updates, conduct a limited exchange of operational reports, and also mutually participate in Emergency Cyber Action Procedures conference calls and other operational coordination forums.

Additionally, DOD and DHS benefit greatly from mutual participation in and support of cyber training exercises. Significant collaboration between the two departments has underpinned the success of the USCYBERCOM-led Cyber Guard and the DHS-led Cyber Storm series of exercises.

In order to further enhance interagency collaboration, streamline information sharing, synchronize operational action, and focus near-term cooperative action, various action plans have been developed between DHS and oraganizations within DOD such as the National Security Agency (NSA) and USCYBERCOM, Examples of these action plans in execution include the Enhance Shared Situational Awareness (ESSA) Information Sharing Architecture (ISA) Implementation Plan and the draft Cyber Action Plan.

○